RESUMEN DE LA SOLUCIÓN

# Acelere considerablemente el tiempo de detección, e interrumpa, investigue y corrija con la solución de Operaciones de Seguridad de Fortinet

## Resumen ejecutivo

No es de extrañar que los actores de amenazas dispongan a menudo de mucho tiempo dentro de una organización para lograr sus objetivos antes de ser detectados. Según la investigación, el equipo de seguridad medio tarda entre 16 y 204 días en detectar un incidente de seguridad en curso.[1] Además, el 75 % de los profesionales de la seguridad afirman que el panorama actual de amenazas es el más difícil de los últimos cinco años.[2]

La solución de operaciones de seguridad de Fortinet utiliza IA y análisis avanzados para supervisar la actividad de los usuarios, dispositivos, redes, correos electrónicos, aplicaciones, archivos y registros, así como para detectar acciones anómalas o malintencionadas que los humanos pueden pasar por alto con facilidad. Además, las integraciones nativas de Fortinet Security Fabric entre componentes permiten el uso compartido de una inteligencia única para la contención automatizada para predecir y limitar el riesgo. Como resultado, los equipos de seguridad cuentan con más tiempo para llevar a cabo una investigación completa y corregir cada incidente de forma automatizada y orquestada, mejorando la eficiencia y la coherencia.

La mitad de las organizaciones afirman que están invirtiendo en IA y ML para detectar amenazas más rápido, y el 44 % señala que utilizan ofertas SIEM y SOAR para mejorar el tiempo de respuesta.[4]

De media, los clientes que utilizan la solución de operaciones de seguridad de Fortinet redujeron el tiempo que necesitan para detectar y contener ataques de 180 horas a menos de una hora (minutos, en la mayoría de los casos), y para posteriormente investigar y corregir entre 10 a 15 minutos.[3]

## La evolución de las amenazas y la ampliación de la superficie de ataque se traducen en vulneraciones más complejas (y costosas)

Con un panorama de amenazas en constante evolución, una superficie de ataque siempre en expansión y una importante escasez de profesionales cualificados, los equipos de seguridad se enfrentan a diario a numerosos desafíos. Debido a ello, incluso los grupos de profesionales mejor dotados y experimentados luchan por proteger con eficacia sus redes corporativas. De acuerdo con el equipo de respuesta a incidentes de FortiGuard —un grupo al que se recurre con frecuencia para investigar ciberataques— los actores de amenazas pasaron desapercibidos en las redes corporativas durante un promedio de 36 días.[5] Una cifra mucho menor a los 204 días que indica un reciente informe de IBM.[6] En cualquier caso, está claro que los actores de amenazas suelen tener mucho tiempo para lograr sus objetivos.

Además, cada vez resulta más costoso mitigar las infracciones. Según una encuesta reciente, el 84% de las organizaciones sufrieron una o más brechas de seguridad en los últimos 12 meses, y el 48% sufrió incidentes cibernéticos cuya corrección costó un millón de dólares o más.[7]

## La solución de operaciones de seguridad de Fortinet acelera la detección y respuesta ante incidentes

En consecuencia, las organizaciones confirman que están priorizando la inversión en tecnologías avanzadas como IA y ML para detectar los signos de intrusión con mayor rapidez, tecnologías centralizadas como SIEM y SOAR para acelerar la respuesta a los incidentes de seguridad, y productos de seguridad integrados para reducir la complejidad.[8]

Por este motivo, la solución de operaciones de seguridad de Fortinet es fundamental para las organizaciones empresariales, ya que ofrece:

- La gama más amplia de sensores basados en el comportamiento, implementados en un dominio específico o en varios dominios, para la detección y la prevención precoz de ciberintrusiones
- Automatización centralizada de la seguridad para agregar, enriquecer y analizar la información de seguridad procedente de esos y otros sensores, así como para visualizar, orquestar y automatizar la investigación y respuesta ante incidentes

- Un conjunto de servicios SOC complementarios para evaluar y mejorar la preparación de las tecnologías y equipos internos, aumentar esos equipos de forma ad hoc o continua, y prestar asistencia en caso de incidentes de crisis
- Asistencia de IA generativa integrada para informar y acelerar las acciones de los analistas en la investigación de amenazas, la estrategia de respuesta y otras actividades clave

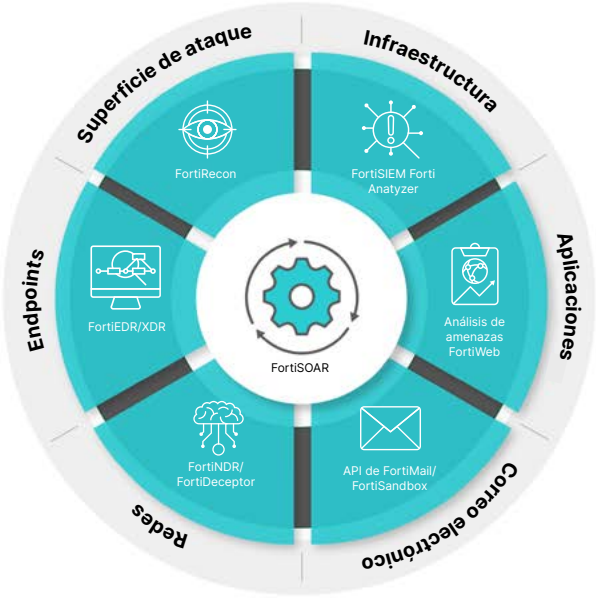


Figura 1: Solución de Operaciones de Seguridad de Fortinet

## La integración permite la automatización con la solución de Operaciones de Seguridad de Fortinet

La solución de Operaciones de Seguridad de Fortinet es una oferta integrada mayor que la suma de sus partes. Además de proporcionar una detección eficaz por sí solos, sus componentes comparten automáticamente información sobre amenazas y toman medidas para que las organizaciones pasen de un modelo de ciberdefensa reactivo a uno proactivo. A continuación se muestran ejemplos de cómo lasolución de Operaciones de Seguridad de Fortinet se integra con otros productos de Fortinet y mejora la seguridad de la organización.

- **FortiEDR:** Después de realizar la detección basada en el comportamiento de actividades de tiempo de ejecución sospechosas o malintencionadas en un dispositivo endpoint y bloquear acciones de alto riesgo, como el cifrado de archivos o el establecimiento de una conexión de red, la integración nativa entre FortiEDR y los NGFW FortiGate permite el intercambio bidireccional de inteligencia sobre amenazas.
- **FortiNDR:** Tras una detección basada en el comportamiento de actividad de red sospechosa o malintencionada de un dispositivo, FortiNDR puede ingerir información del dispositivo desde FortiEDR e incluso activar una cuarentena del dispositivo de origen gracias a su integración nativa.
- **FortiRecon:** Después de evaluar los activos externos, la integración nativa de FortiRecon le permite recibir activos adicionales de los NGFW FortiGate para incluirlos en el inventario y análisis de activos.
- **FortiDeceptor:** Una vez detectada la intrusión de un actor de amenaza, la integración nativa permite a FortiDeceptor dirigir los NGFW FortiGate para bloquear el acceso a otros dispositivos al tiempo que devuelve las respuestas esperadas del dispositivo para continuar involucrando al atacante desconocido.
- **FortiSandbox:** Después de hacer una clasificación del riesgo basada en el comportamiento, FortiSandbox puede compartir esa clasificación con muchos dispositivos Fortinet, incluidos NGFW FortiGate y FortiMail, para el bloqueo en tiempo real antes de la entrega.
- **FortiAnalyzer:** Una integración nativa con la amplia cartera de soluciones de Fortinet permite a las organizaciones establecer activadores de eventos y respuestas de automatización.
- **FortiSIEM:** Después de realizar detecciones mediante un conjunto enriquecido de análisis, incluidos los de un entorno de trabajo ML, los incidentes pueden gestionarse a través de acciones de corrección habilitadas por más de 300 integraciones tecnológicas o transferidas sin problemas a FortiSOAR para una orquestación y automatización sólida.

- **FortiSOAR:** Una vez que FortiSOAR recibe alertas sobre actividades sospechosas, se pueden llevar a cabo acciones automatizadas, como la implementación de herramientas de engaño en la ubicación correcta para embaucar y detener al actor de la amenaza.

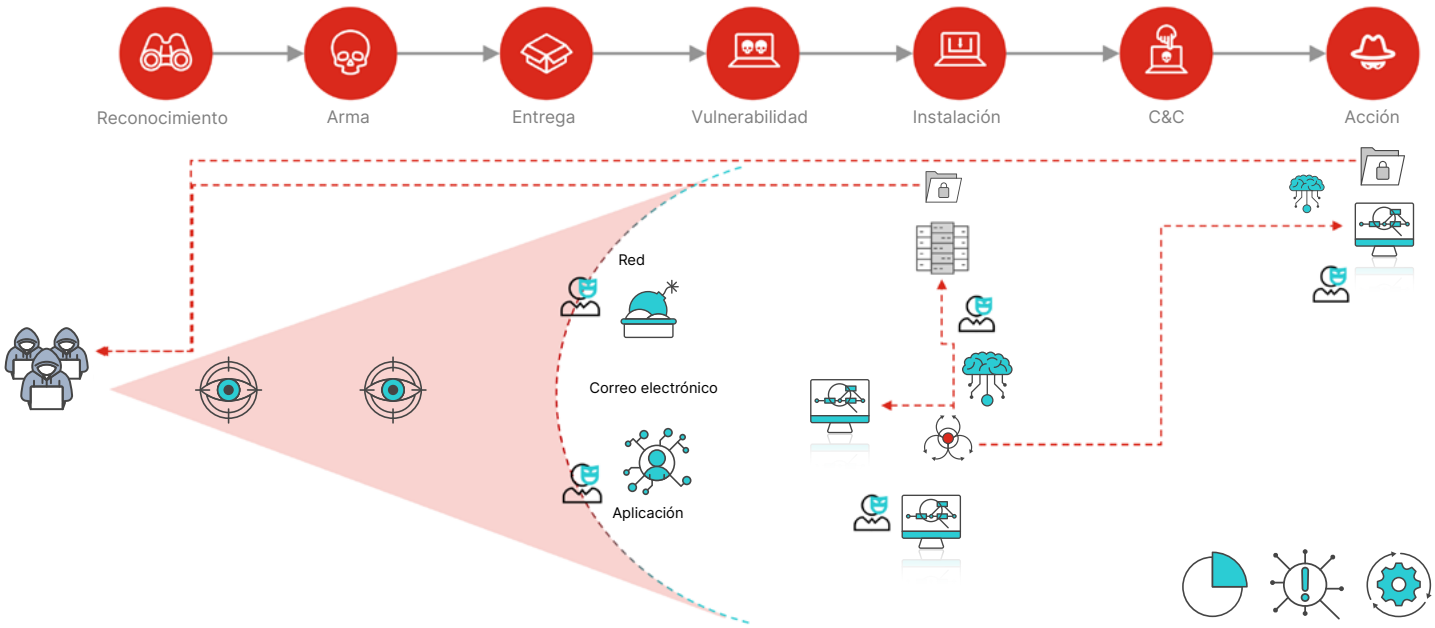


Figura 2: Componentes de la solución de Operaciones de Seguridad de Fortinet aplicados a lo largo de la cadena de ataque

## Los clientes que utilizan la solución de Operaciones de Seguridad de Fortinet obtienen un retorno de la inversión del 597 %[9]

Se ha demostrado que la inversión en los componentes de la solución de Operaciones de seguridad de Fortinet reduce drásticamente el tiempo de exposición, el ciber riesgo y el esfuerzo de las operaciones de seguridad. De manera específica:

- Antes de realizar inversiones en sensores de detección temprana y prevención, los clientes de Fortinet señalaron que, de media, sus equipos tardaban 21 días en detectar intrusiones cibernéticas y un día y medio más en contenerlas.[10] Sin embargo, tras implementar productos como FortiEDR, FortiNDR y FortiDeceptor, entre otros, indicaron que tenían capacidad para detectar y contener en una hora (y en minutos para la mayoría) la actividad de los actores de amenazas.[11]
- Antes de implementar los componentes de la solución de Operaciones de Seguridad de Fortinet, las organizaciones informaron de que la investigación y corrección de alertas tardaba de dos a tres días.[12] Después de implementar componentes, como FortiAnalyzer, FortiSIEM, FortiSOAR u otros, las investigaciones podían completarse en 10-15 minutos.[13]
- Además, los clientes informaron de que un equipo de seis personas (o incluso tres, en un caso) podía realizar el trabajo de 12, lo que suponía una mejora espectacular de la eficiencia operativa.[14]


Figura 3: Ventajas cuantificadas de la implementación de los componentes de Operaciones de Seguridad de Fortinet

ESG Research cuantificó el valor de estas mejoras en relación con la reducción de riesgos y los beneficios financieros previstos. La investigación muestra que una organización media tiene casi un 30 % de probabilidades de sufrir una brecha en un año determinado, lo que supone un coste anual previsto de 1,4 millones de dólares.[15] Combinado con el menor tiempo que se tarda en detectar e interrumpir, investigar y corregir, ESG Research calculó un ahorro anual de 1,39 millones de dólares en cuanto a la reducción de los costes previstos de las brechas mediante la implementación de componentes de la solución de Operaciones de Seguridad de Fortinet.[16]

Además, como resultado del aumento de la productividad tras la implementación de la solución, se prevé que los equipos de seguridad ahorren una media de 1,9 millones de dólares en costes de personal.[17] En última instancia, ESG Research estima un retorno de la inversión del 597% para las organizaciones que inviertan en la solución de Operaciones de Seguridad de Fortinet, con un periodo de amortización de menos de dos meses.[18]

## Conclusión

La solución de Operaciones de Seguridad de Fortinet permite a las organizaciones incorporar capacidades de detección eficaces basadas en IA en toda su organización digital e integrarse con los controles de seguridad existentes para reducir notablemente el tiempo que se tarda en interrumpir los ciberataques a lo largo de la cadena de ataque. La solución también permite a los equipos de seguridad orquestar, automatizar y aumentar los esfuerzos centralizados de investigación y corrección de incidentes para lograr una respuesta más rápida y coherente. Por último, proporciona servicios adicionales de expertos para evaluar la preparación de las operaciones de seguridad y ayudar en la respuesta a incidentes de seguridad cuando sea necesario. Esta amplitud de cobertura y profundidad de integración de la solución de Operaciones de Seguridad de Fortinet ayuda a los equipos de seguridad a cambiar su enfoque de "detectar y responder", que consume mucho tiempo, por un paradigma más rápido para una ciberdefensa activa basado en "detectar e interrumpir, después investigar y corregir".

1 Cost of a Data Breach Report 2023, IBM, 24 de julio de 2023.

2 How the Economy, Skills Gap, and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, ISC2, 31 de octubre de 2023.

3 Validación económica de ESG: The Quantified Benefits of Fortinet Security Operations Solutions, Enterprise Strategy Group, 1 de agosto de 2023.

4 2023 Global Ransomware Report, Fortinet, 20 de abril de 2023.

5 FortiGuard Labs, acceso del 21 de noviembre de 2023.

6 Cost of a Data Breach Report 2023, IBM, 24 de julio de 2023.

7 2023 Global Cybersecurity Skills Gap Report, Fortinet, 21 de marzo de 2023.

8 2023 Global Ransomware Report, Fortinet, 20 de abril de 2023.

9 ESG Economic Validation: The Quantified Benefits of Fortinet Security Operations Solutions, Enterprise Strategy Group, 1 de agosto de 2023.

10-18 Ibid.





febrero 22, 2024 1:52 p.m.
2431037-0-0-ES