# Fortinet Customer Experience (FCE)

Análisis de ciberseguridad por especialistas

Detalles del beneficio

Año: 2020

# Índice

## Acerca de Fortinet

Producto de la innovación Fortinet (FTNT) nace en el año 2000 desarrollando equipamiento específico dedicado a mitigar los problemas de seguridad de red y desde entonces se ha posicionado como una de las empresas líderes, siendo hoy reconocida como la marca número 1 en despliegue de soluciones de ciberseguridad.


Recomendada mundialmente por los principales analistas, con más de 455.000 clientes a nivel mundial y 30 líneas de soluciones, Fortinet aprovecha su experiencia y recursos enfocado en entregar mejores soluciones y servicios día a día.

## Fortinet Customer Experience (FCE)

Como su nombre lo indica, FCE es una iniciativa de la marca que tiene como objetivo ofrecer una experiencia diferente, otorgando un beneficio único que le permite a sus mayores clientes disponer de un especialista calificado que lo asesore en mejores prácticas de ciberseguridad. Como resultado de dicho análisis se entregarán una serie de recomendaciones que permitirán optimizar el uso de las diferentes soluciones de red y ciberseguridad del cliente, así como también analizar métricas referentes al nivel de exposición a amenazas más comunes.

## Alcance

El beneficio cubre dos tipos de necesidades:

- Análisis de red y mejores prácticas
- Exposición a amenzas de ciberseguridad

**Análisis de red y mejores prácticas:** El especialista se concentrará en las diferentes soluciones desplegadas en la red (foco en los productos Fortinet), atendiendo a los detalles de configuración, versiones, topología, etc. Como resultado se entregará un completo informe con recomendaciones, sugerencias, ajustes, propuestas de mejora y optimización de recursos.

**Exposición a amenazas de ciberseguridad:** El especialista se concentrará en este punto en las soluciones y arquitecturas requeridas para mitigar el campo de acción de diferentes flagelos informáticos como ser el Malware, DDoS, Phishing, etc.. Como resultado se entregará un completo análisis con ponderación de nivel de exposición, recomendaciones y sugerencias enfocadas a mitigar las diferentes amenazas, basado en un modelo de maduración NIST.

**Especialistas Asignados:** Para las mencionadas tareas Fortinet pondrá a disposición a sus equipos técnicos de ingeniería y arquitectura de soluciones. En función del cliente y de la especialización requerida, el técnico asignado podrá variar, por lo que se informará en cada caso, el nombre del responsable a asignar, su rol, formación y experiencia en ciberseguridad.

## Campo de Acción

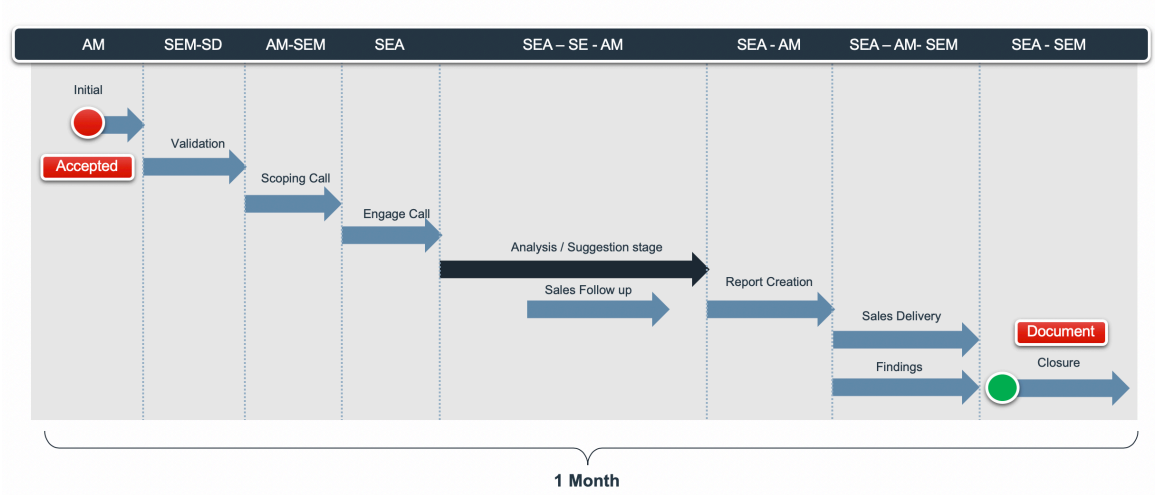
El proceso de relevamiento será del tipo remoto, el equipo de especialistas asignado se contactará con el cliente a fin de relevar las necesidades iniciales y comenzar con el análisis. Para dicho proceso, se intercambiará información en formato cuestionario y se estipularán diferentes reuniones en la cuales los responsables irán despejando dudas y recopilando diferentes datos. Las reuniones serán programadas con antelación y durarán un tiempo variable en función del tamaño del cliente y alcance del servicio a entregar.

El proceso de relevamiento puede variar en función del beneficio asignado. Para el caso de exposición al ransomware, los ítems a analizar se concentran en lo siguiente:

| Item | Descripción |
|---|---|
| **Acceso Remoto** | Evaluaremos potenciales usuarios vulnerables y su proceso de conexión a redes corporativas. Tipo de VPN utilizadas, portales SSL o RDP, tipo y mecanismos de autenticación utilizados, control de postura y remediación de endpoints vulnerados. |
| **Correo electrónico** | Mas del 90% de los ataques de ransomware utilizan el correo electrónico como mecanismo de contagio. Evaluaremos detenidamente las soluciones AntiSPAM, tipo y sistemas de correo electrónico, protección activa de phishing y filtrado de contenido embebido. |
| **Flujos de información** | La información distribuida puede ser un problema grave a la hora de enfrentar y controlar el malware. Analizaremos detalles de dominio, autenticación, repositorios y sistemas centrales de información, tanto locales como en nube. Para este último caso evaluaremos controles específicos (shadow IT). |
| **Controles Avanzados** | El ransomware opera silenciosamente, pero muestra señales que son importantes detectar a tiempo para mitigar la amenaza antes de que sea demasiado tarde. Evaluaremos controles disponibles en la red para detectar anomalías conocidas y ataques de día cero. Analizaremos el alcance de la inspección profunda y cifrada en soluciones tales como NGFW, IPS, Sistemas de inteligencia artificial, NGAV, Sandbox, EDR, DNS filter, endpoint control, etc. |
| **Segmentación** | A fin de detener el movimiento lateral por el cual el malware se propaga, buscaremos barreras internas conocidas como firewall de segmentación (ISFW) y analizaremos su rol en la micro-segmentación. |
| **Entrenamiento** | El contagio utiliza en un 90% de los casos el engaño a usuarios finales. Los mecanismos de control no siempre son eficaces por lo cual es importante capacitar y formar al personal en materia de ciberseguridad. Evaluaremos el conocimiento general de los usuarios sobre SPAM y phishing. Analizaremos herramientas, frecuencias y mecanismos de capacitación utilizados. |
| **Hardening** | En pos del funcionamiento inmediato, los ajustes de configuraciones relativas a ciberseguridad son muchas veces ignorados lo que produce puertas de entrada a numerosos ataques. Consultaremos sobre el nivel de parchado de activos críticos, analizaremos el manejo de usuarios de administración, política de contraseñas, timeout de sesiones, etc. |
| **Contingencia** | Ante la imposibilidad de detener un posible ataque, analizaremos los planes de acción y remediación. |

## Detalles del proceso

La tarea contempla numerosas etapas que comienzan con el comunicado formal del beneficio al cliente final y finalizan con la entrega del informe. A continuación, se detallan cada uno de sus pasos.




**Initial:** A fin de evaluar el interés, los clientes proclives al beneficio serán contactados e informados de dicho beneficio.

**Validation:** Si el cliente está de acuerdo en avanzar con el análisis, se designará un equipo de trabajo y se recopilará información sobre las necesidades básicas a cubrir.

**Scoping Call:** En este punto el equipo asignado (AM/SEM/SD) se comunicará con el cliente a fin de definir los alcances de la tarea y los interlocutores técnicos válidos para realizarla.

**Engage Call:** El ingeniero a cargo (SE/SEA) se contactará con los técnicos responsables para así comenzar con el trabajo.

**Analysis:** El ingeniero a cargo comenzará su tarea de relevamiento e investigación, dialogará con el equipo técnico del cliente y con sus contrapartes de ingeniería (SE) con el objetivo de obtener un detalle completo de la red, historia, problemáticas y necesidades del cliente.

**Report Creation:** El ingeniero a cargo trabajará en la creación del reporte final con sugerencias, recomendaciones de mejora, matrices de ponderación y exposición a diferentes amenazas.

**Report Delivery:** El equipo de trabajo sostendrá una reunión de presentación del informe con todos los responsables del cliente.

**Closure:** Se analizarán los resultados finales y se entregarán las últimas recomendaciones y el informe completo.

NOTAS:

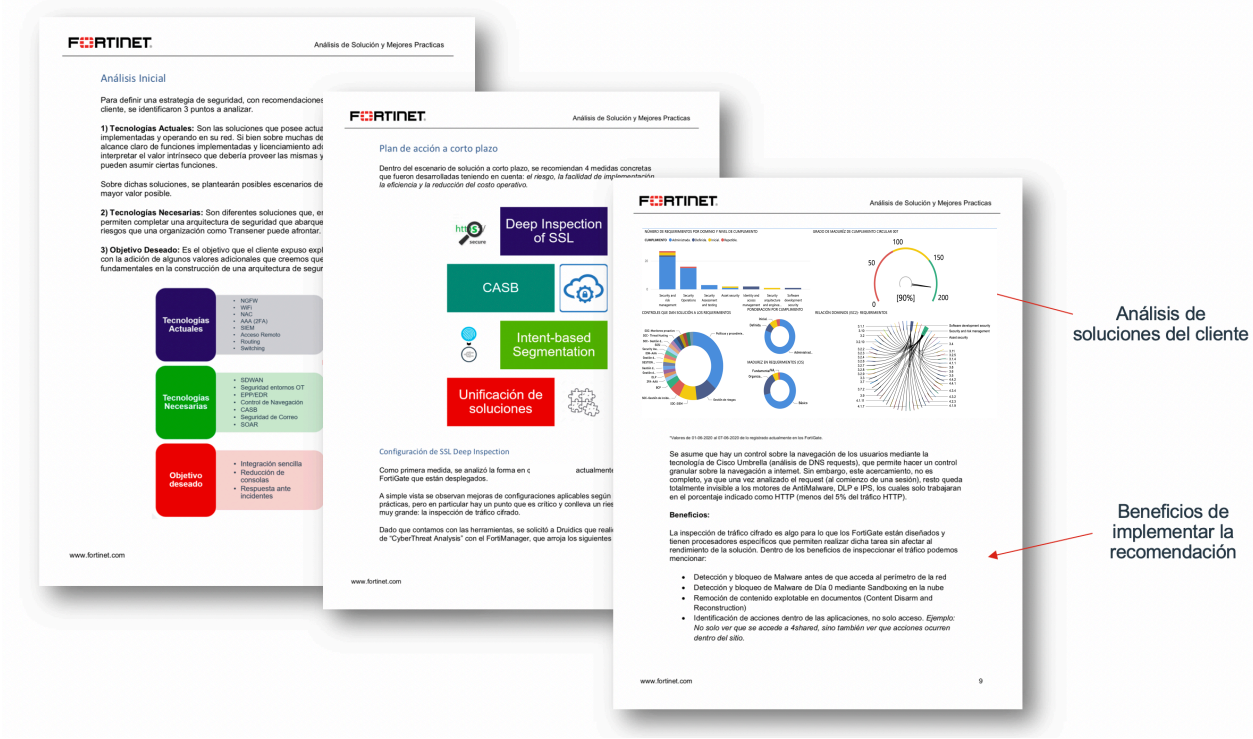
- Dependiendo del tipo de beneficio, las tareas pueden demorar entre 7 y 30 días.
- La duración de las tareas está sujeta; entre otras cosas, a la disponibilidad del cliente.
- Nomenclatura, Fortinet: AM (ejecutivo de cuentas), SEM (Manager de ingeniería), SD (Director de ventas), SE (Ingeniero especialista), SEA (Ingeniero Arquitecto)

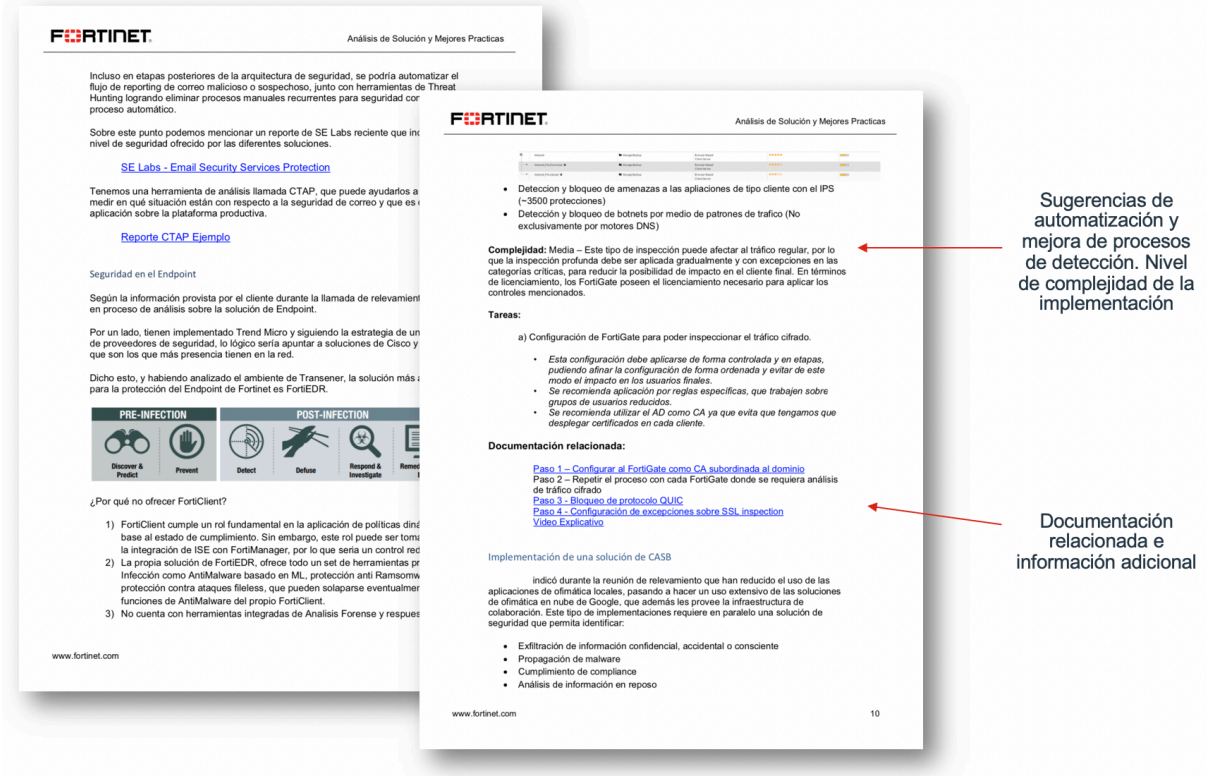
## Estructura Básica del reporte entregado

La iniciativa FCE ofrece un completo reporte final que contiene en líneas generales la siguiente información:

- Detalles de FCE y del especialista SEA asignado
- Plan de trabajo
- Minutas y resúmenes de las reuniones sostenidas
- Análisis de red (tecnologías actuales y sugeridas)
- Puntos de mejora (reconfiguración y ajustes)
- Análisis gráfico de riesgo basado en NIST
- Propuesta de solución integral
- Planes de acción
- Próximos pasos
- Anexos e información adicional

A continuación, se muestran algunas imágenes del mencionado reporte y presentaciones al cliente:




NOTAS: La estructura del reporte puede variar en función del beneficio asignado.

## Confidencialidad:

Las tareas a realizarse se acuerdan exclusivamente entre el cliente, el integrador y Fortinet. En caso de ser requerido se podrá evaluar la firma de un acuerdo de confidencialidad que garantice la no divulgación de la información recopilada. En todos los casos los pormenores de este punto podrán ser evaluados en la reunión inicial de alcance (Scopping call).