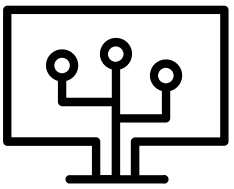

F-SECURE
DETECCIÓN RÁPIDA Y RESPUESTA

Descripción de la Solución

F-Secure

Tabla de Contenidos

ACLARACIÓN:

Este documento ofrece una descripción general de alto nivel de los componentes de seguridad clave en la solución F-Secure Rapid Detection & Response. Los detalles se omiten para evitar ataques dirigidos contra nuestras soluciones.

F-Secure está mejorando constantemente sus servicios. F-Secure se reserva el derecho de modificar las características o la funcionalidad del Software de acuerdo con sus prácticas de ciclo de vida del producto.

1. RESUMEN EJECUTIVO

Los ataques dirigidos a la ciberseguridad pueden ser difíciles de analizar y responder, y convertirse en un problema extremadamente costoso para las empresas, incluso antes de que se conviertan en violaciones de datos reales. La etapa de remediación de ataques por sí sola puede durar más de un mes y costar casi un millón de dólares (1. Los ataques sin archivos generalmente no son reconocidos por la protección antivirus tradicional, y los ataques dirigidos a menudo pasan desapercibidos durante meses o incluso años) Solución de detección y respuesta: puede obtener una visibilidad contextual de su seguridad, automatizar la identificación de amenazas y detener los ataques antes de que ocurran las violaciones de datos.

F-Secure Rapid Detection & Response (RDR) es una solución líder de detección y respuesta de puntos finales a nivel de contexto (EDR) para ayudar a las empresas a obtener una visibilidad inmediata de su entorno de TI y seguridad, proteger la empresa y sus datos confidenciales mediante la detección de ataques rápidamente , y respondiendo rapido con guia de expertos. Con su profunda inteligencia bidireccional y su alto nivel de automatización, la solución de F-Secure protege contra amenazas avanzadas incluso antes de que ocurran las violaciones. Detecta incidentes con clientes ligeros, que se instalan en hosts monitoreados en toda la red de la organización. Los clientes recopilan datos sobre eventos de comportamiento, como acceso a archivos, procesos iniciados, conexiones de red que se crean o algo que se escribe en el registro o en los registros del sistema. Estos eventos son luego analizados por la solución. Además de las detecciones en tiempo real, la solución también realiza detecciones basadas en datos históricos.

EL SERVICIO EDR GESTIONADO POR EL SOCIO

La solución está disponible como un servicio EDR gestionado por el socio que combina tecnología, inteligencia de amenazas y servicios del socio para proporcionar un servicio de detección y respuesta de violaciones de todo en uno. Los servicios EDR administrados liberan los recursos propios de una organización del control avanzado de amenazas y la gestión de incidentes para alertar a la organización solo cuando se detectan amenazas reales. El servicio está respaldado por F-Secure, lo que significa que una detección puede ser elevada a F-Secure para un análisis de amenazas adicional por expertos en seguridad cibernética.

Al final del día, utilizar tecnología de punta es solo una parte de la ecuación, ya que la tecnología es tan buena como la gente que la respalda. Nuestros cazadores de amenazas e investigadores se encuentran entre los principales expertos en la industria y están inmensamente dedicados a brindar lo mejor en el mercado de la ciberseguridad. En F-Secure, combinamos esa tecnología y esa experiencia humana insuperable para ofrecer una solución de respuesta y detección de puntos finales de clase mundial.

[1] Ponemon Institute's 2016 Cybersecurity Trend Report's 252 surveyed participants said that they took an average of 45 days to resolve a cyberattack which translates to spending about $973,000 during the attack remediation stage alone.
[2] Gartner 2017 reported 99 days in the Americas; Ponemon Institute's 2016 Cybersecurity Trend Report stated 98 days for financial companies and 197 days for retailers.

2. BENEFICIOS CLAVE

Con la solución F-Secure Rapid Detection & Response, puede estar preparado para detectar amenazas avanzadas y ataques dirigidos antes de que ocurran las violaciones de datos, y siempre estar listo para analizarlos rápidamente y responder a ellos utilizando la tecnología de vanguardia de F-Secure.

A continuación se enumeran algunos de los beneficios clave que ofrece la solución para la visibilidad, detección y respuesta:.

VISIBILIDAD	DETECCIÓN	RESPUESTA
Visibilidad contextual inmediata en el entorno de TI y el estado de seguridad	Proteja su negocio y sus datos confidenciales detectando brechas de datos rápidamente	Responde rápidamente con la ayuda de la automatización y la guía cuando te encuentres bajo ataque

1. **Obtenga visibilidad contextual inmediata de su entorno de TI y estado de seguridad**
   - Mejorar la visibilidad en el estado del ambiente y la seguridad con la aplicación y los inventarios de puntos de referencia
   - Detecta fácilmente el uso indebido del uso adecuado mediante la recopilación y la correlación de eventos de comportamiento más allá del malware
   - Responda a los mensajes de texto para identificar el objetivo del ataque, gracias a las alertas con un amplio contexto y su crítica
2. **Proteja su negocio y sus datos confidenciales detectando violaciones rápidamente**
   - Detectar y detener los portaequipajes rápidamente para evitar interrupciones en el negocio y afectar la reputación de la empresa
   - Prepárese antes de que se abran los sucesos.
   - Cumplir con los requisitos reglamentarios de PCI, HIPAA y el GDPR de la Unión Europea que requiere que se notifiquen las violaciones de datos dentro de las 72 horas
3. **Responda rápidamente con la automatización y la guía cuando esté bajo ataque**
   - Mejorar el enfoque de su equipo con la automatización incorporada y sus comienzos para responder mejor a las amenazas avanzadas reales y los ataques dirigidos.
   - Reciba la guía en los comercios y responda cuando se produzcan correcciones, con la opción de automatizar las acciones de respuesta durante todo el día (se espera que la automatización esté disponible más adelante en el H2 / 2018)
   - Superar los recursos de la memoria o los recursos de los equipos por medio de la subcontratación y supervisar el seguimiento a un proveedor de servicios gestionados certificado por F-Secure respaldado por expertos de F-Secure

3. DESCRIPCIÓN GENERAL DE LA SOLUCIÓN

La solución F-Secure Rapid Detection & Response (RDR) consiste en una combinación de clientes fácilmente implementables en hosts, un Portal de administración basado en la nube y servicios administrados opcionales de socios certificados. La solución proporciona funcionalidad para detectar amenazas avanzadas y ataques dirigidos, y Detecciones de contexto amplio para aclarar el riesgo y la respuesta general. La parte en el sitio de la implementación incluye el cliente de respuesta y monitoreo de puntos finales que se instala en los puntos finales de una organización.

Figura 1: Descripción general de la solución F-Secure Rapid Detection & Response

La figura anterior describe en un alto nivel cómo funciona la solución F-Secure Rapid Detection & Response:trabaja:

1. Los **clientes ligeros** monitorean diferentes actividades de punto final que realizan los atacantes y transmiten eventos de comportamiento a nuestra nube en tiempo real.

2. El **análisis de datos de comportamiento en tiempo real** marca y supervisa tanto los procesos como otros comportamientos que han desencadenado los eventos.

3. Los **mecanismos de Detección de contexto amplioTM** reducen aún más los datos, colocan los eventos relacionados en contexto entre sí, identifican rápidamente los ataques reales y los priorizan con respecto al nivel de riesgo, la criticidad del huésped y el panorama de amenazas prevaleciente.

4. Tras una **detección confirmada, la solución guía a los equipos** de TI y de seguridad a través de los pasos necesarios para contener y remediar la amenaza.

3.1 portal de gestión

La solución de detección y respuesta rápida facilita la implementación, administración y monitoreo de las amenazas avanzadas en sus puntos finales desde una única consola intuitiva basada en la web. Le brinda visibilidad contextual inmediata del entorno de TI y del estado de seguridad en su red, independientemente de si los empleados están en la oficina o en cualquier lugar.

El portal de administración fue diseñado para simplificar y acelerar la administración de la seguridad en entornos exigentes y de sitios múltiples. A continuación, se incluyen algunos ejemplos de cómo la solución reduce considerablemente la cantidad de tiempo y recursos necesarios para el monitoreo y la gestión avanzados de amenazas:

- La solución está diseñada para funcionar con cualquier solución de protección de punto final y funciona con las soluciones de seguridad de punto final de F-Secure en una infraestructura de administración y cliente único.
- Cuando se combina con F-Secure Protection Service para empresas (PSB), tanto el malware como las amenazas avanzadas se vuelven visibles y manejables (se espera en el cuarto trimestre de 2018).
- Las detecciones se presentan con visualización accionable para proporcionar un contexto más amplio de ataques dirigidos en una línea de tiempo con todos los hosts afectados, eventos relevantes y acciones recomendadas.
- Al consolidar la gestión avanzada de amenazas de puntos finales y herramientas del sistema en un portal de seguridad de puntos finales, la administración general se agiliza considerablemente, ahorrando tiempo.
- Como se trata de un servicio basado en la nube administrado por F-Secure, no es necesario instalar ni mantener ningún hardware o software de servidor; todo lo que necesita es un navegador y una conexión a Internet.

El portal de administración es compatible con las últimas versiones de los siguientes navegadores: Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome y Safari. El Portal está disponible en alemán, inglés, francés, japonés y polaco (a partir de septiembre de 2018).

La versión del portal de administración administrada por el socio incluye características específicamente diseñadas para ayudar a los proveedores de servicios, como los informes de los clientes finales, un panel de control con una visión general conveniente de todas las compañías que administran, y también el acceso al panel de control de cada compañía administrada.

3.2 clientes de punto final

Los clientes de punto final son herramientas de monitoreo livianas y discretas diseñadas para la detección de anomalías, implementables en todas las computadoras Windows y MacOS relevantes dentro de la organización. Los clientes recopilan datos de eventos de comportamiento de los puntos finales, están diseñados para funcionar con cualquier solución de protección de puntos finales y funcionan a la perfección con las soluciones de seguridad de puntos finales de F-Secure en una infraestructura de administración basada en la nube y para un solo cliente.

La tabla a continuación describe los sistemas operativos compatibles y las características de cada sistema operativo.

	WINDOWS WORKSTATIONS	WINDOWS SERVERS	MAC OS
OPERATING SYSTEMS	7 / 8 / 10	2018 R2 / 2016 / 2012 R2 / 2012	10.11 or newer
SINGLE-CLIENT WITH F-SECURE	YES*	NO**	YES*
CLIENT WITH COMPETITIVE EPP	YES	YES	YES
BEHAVIORAL EVENTS	YES	YES	YES
APPLICATION VISIBILITY	YES	YES	NO**
REMOTE HOST ISOLATION	YES	YES	NO**

*** Limited support:** Initially only with Computer Protection from F-Secure Protection Service for Business (PSB). Please confirm client compatibility with the existing version, e.g. Protection Service for Business must be upgraded to Computer Protection.
** **Expected later:** The feature is not available in the GA release but it will be supported later.

Además del Servicio de Protección F-Secure para Empresas (Protección de Computadoras), la compatibilidad de la solución se ha probado con las siguientes soluciones de protección de puntos finales (desde agosto de 2018): Bitdefender Endpoint Security Tools, ESET Endpoint Security; Kaspersky Endpoint Security; McAfee Endpoint Security; Microsoft Windows Defender; Panda Adaptive Defense 360; Trend Micro Business Security; Sophos Endpoint Security and Control, Symantec Endpoint Protection y Webroot SecureAnywhere.

3.3 Visibilidad de la aplicación

Obtener una amplia visibilidad de su entorno de TI y sus servicios en la nube reducirá la exposición a amenazas avanzadas y fugas de datos. La visibilidad de la aplicación de nuestra solución le permite enumerar todas las aplicaciones activas que se ejecutan en los puntos finales de la red de su organización para que pueda identificar fácilmente las aplicaciones no deseadas, desconocidas y dañinas.

Con la visibilidad de la aplicación, puede identificar Aplicaciones potencialmente no deseadas (PUA) y Aplicaciones no deseadas (UA). Las "aplicaciones potencialmente no deseadas" tienen comportamientos o rasgos que puede considerar indeseables o no deseados. Las 'Aplicaciones no deseadas' tienen comportamientos o rasgos con un impacto más severo en su dispositivo o datos.

Las aplicaciones identificadas como 'Potencialmente no deseadas' (PUA) pueden:

- Afectar su privacidad o productividad, por ejemplo, exponer la información personal o realizar acciones no autorizadas.
- Poner un estrés excesivo en los recursos de su dispositivo, por ejemplo, use una cantidad excesiva de almacenamiento o memoria
- Compromiso con la seguridad de su dispositivo y la información almacenada en su cuenta por ejemplo, lo expone a contenido o aplicaciones inesperados

El impacto de estos comportamientos y rasgos en su dispositivo o datos puede variar de leve a grave. Sin embargo, no son lo suficientemente dañinos como para justificar la clasificación de la aplicación como malware.

3.4 Análisis de comportamiento

Como una funcionalidad central para identificar amenazas avanzadas entre cantidades masivas de eventos de datos de comportamiento, F-Secure utiliza el análisis de comportamiento, reputación y big data en tiempo real con aprendizaje automático para recopilar múltiples eventos sospechosos que pueden vincularse, por ejemplo, según actividades .

El análisis de comportamiento aprovecha la inteligencia artificial para detectar actividades maliciosas y ocultas basadas en pequeños eventos individuales que se ejecutan como parte de las tácticas, técnicas y procedimientos del atacante.

La inteligencia artificial incluye capacidades de aprendizaje automático que se aplican para mejorar continuamente las detecciones y reducir los falsos positivos. Las capacidades de análisis de comportamiento son un excelente ejemplo en el que F-Secure combina la experiencia en ciencia de datos y seguridad cibernética, un enfoque que F-Secure denomina "Hombre y Máquina".

3.5 Detección de contexto amplio

Las metodologías patentadas de detección de contexto amplio de F-Secure están diseñadas para reducir el número de detecciones a un pequeño número de incidentes significativos.
Broad Context DetectionTM señala las indicaciones de posibles infracciones al alertar a los administradores de tácticas, técnicas y procedimientos (TTP) utilizados en ataques dirigidos. Esto puede incluir, por ejemplo, las siguientes acciones posiblemente sospechosas:

• Actividad anormal de los programas estándar.
• Llamadas a procesos en ejecución desde ejecutables no estándar.
• Ejecución de scripts inesperados
• Ejecución inesperada de herramientas del sistema a partir de procesos estándar
.
Broad Context DetectionTM solo muestra detecciones relevantes y les asigna una criticidad basada en el nivel de riesgo, la información sobre los hosts afectados y el panorama de amenazas prevaleciente.
Como resultado de este enfoque, a los equipos de TI se les proporciona una lista relativamente corta de detecciones confirmadas, cada una marcada con distintos niveles de prioridad y acciones de respuesta recomendadas. Así que no solo los equipos saben en qué concentrarse primero, sino que también saben cómo responder y pueden hacerlo de manera rápida y decisiva.