LAS BRECHAS DE SEGURIDAD SUCEDEN:
PREPÁRESE

PROTEJA SUS DATOS Y SU “INFORMACIÓN” CONTRA ATAQUES AVANZADOS

La prevención efectiva de amenazas previas al compromiso es la piedra angular de la seguridad cibernética, pero no puede confiarse únicamente en las medidas preventivas para mantener su negocio y sus datos a salvo de las tácticas, técnicas y procedimientos que los adversarios utilizan en ataques dirigidos.

El panorama de amenazas en continua evolución, junto con las exigencias regulatorias como GDPR, requieren que las empresas estén preparadas para la detección de infracciones posteriores al compromiso. Eso significa garantizar que una empresa sea capaz de responder rápidamente a los ataques avanzados.

La solución de F-secure, entrenada por un equipo experimentado de caza de amenazas, monitorea su estado de seguridad a través del análisis de comportamiento infundido con la última inteligencia de amenazas. Con sus actividades de detección y respuesta gestionadas por proveedores de servicios certificados, puede concentrarse en su negocio y contar con la orientación de expertos cuando se encuentra bajo ataque.

DETENGA BRECHAS RÁPIDAMENTE CON GUÍA

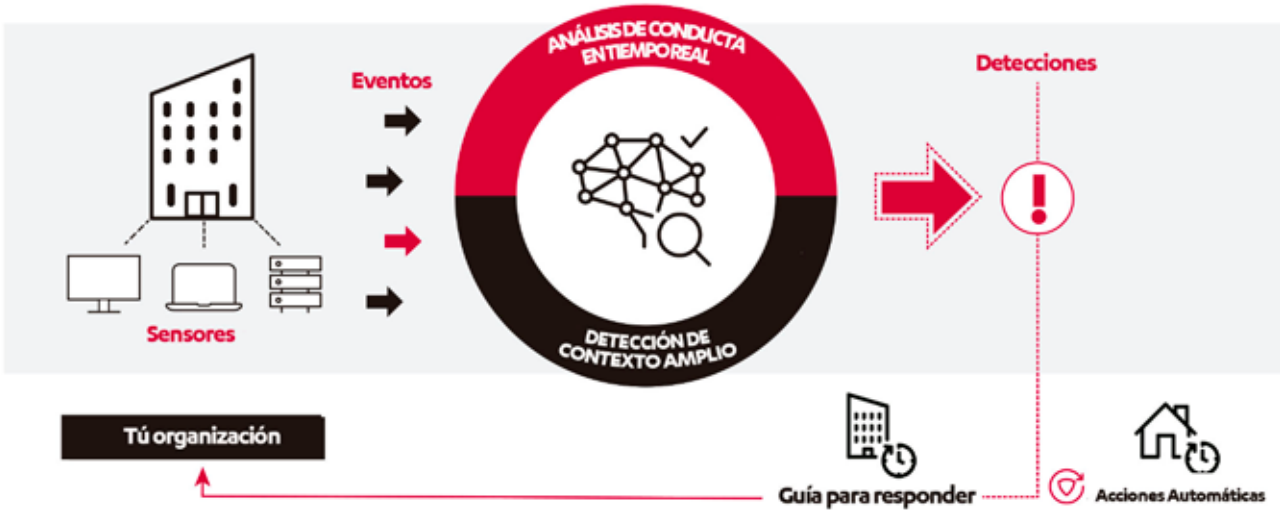
Necesita tanto la mejor tecnología como la última experiencia humana para proteger a su organización contra las amenazas cibernéticas avanzadas.

La solución de detección y respuesta de puntos finales (EDR) de Fsecure le brinda visibilidad contextual de amenazas avanzadas, lo que le permite detectar y responder a ataques dirigidos con automatización y orientación.

.

Cuando se produce una violación, necesita algo más que una alerta. Para planificar la mejor respuesta posible, debe comprender los detalles del ataque.

Nuestros mecanismos de Detección de contexto amplio, junto con los proveedores de servicios certificados y la automatización incorporada, detendrán el incumplimiento y brindarán consejos útiles para acciones de remediación futuras.



LA TECNOLOGÍA LÍDER DE LA INDUSTRIA DE F-SECURE A SU SERVICIO

1. Los sensores ligeros implementados en los puntos finales monitorean los eventos de comportamiento generados por los usuarios y los transmiten a nuestra nube en tiempo real

2. Nuestro análisis de datos de comportamiento en tiempo real y los mecanismos de Detección de Contexto Amplio reducen los datos, distinguiendo el comportamiento malicioso para identificar de manera rápida los ataques reales.

3. Tras una detección confirmada, la solución proporciona consejos y recomendaciones para guiarlo a través de los pasos necesarios para contener y remediar la amenaza.

EN BUSCA DE UNA AGUJA EN UN EJEMPLO DE HAYSTACK-MUNDO REAL

En una instalación de cliente de 325 nodos, nuestros sensores recolectaron alrededor de 500 millones de eventos en un período de un mes. El análisis de datos sin procesar en nuestros sistemas de back-end filtró ese número hasta 225,000 eventos.

Nuestros mecanismos de Detección de Contexto Amplio analizaron los eventos sospechosos para reducir el número de detecciones a solo 24. Finalmente, esas 24 detecciones fueron revisadas en detalle, con solo 7 confirmadas como amenazas reales.

Enfocarse en detecciones menos precisas permite acciones de respuesta más rápidas y efectivas cuando se está bajo un ataque cibernético real.

500 MILLONES

Datos de eventos / mes

Recogido por 325 sensores de punto final

225 000

EVENTOS SOSPECHOSOS

Después del análisis de comportamiento en tiempo real de los eventos.

24

DETECCIONES

Después de agregar un contexto más amplio a los eventos sospechosos

7

AMENAZAS REALES

Después de confirmar las detecciones como amenazas reales.

VISIBILIDAD

Obtenga visibilidad inmediata de su entorno de TI y estado de seguridad

Mejora la visibilidad del entorno de TI y el estado de seguridad a través del inventario de aplicaciones y puntos finales.

Identifica la actividad sospechosa mediante la recopilación y correlación de eventos de comportamiento más allá del malware estándar

Proporciona alertas con amplia información de contexto y criticidad de activos, facilitando la respuesta a incidentes

DETECCION

Proteja su negocio y sus datos confidenciales detectando brechas rápidamente

Detecte y detenga los ataques dirigidos rápidamente para minimizar las interrupciones del negocio y el impacto negativo de la marca.

La solución está disponible en horas, lo que le permite estar listo para las infracciones de inmediato.

Cumplir con los requisitos reglamentarios de PCI, HIPAA y GDPR que requieren que se notifiquen las infracciones dentro de las 72 horas

RESPUESTA

Responde rápidamente con la guía de un experto cuando esté bajo ataque.

La automatización e inteligencia incorporadas ayudan a su equipo a enfocarse solo en ataques reales.

Las alertas incluyen una guía de respuesta adecuada, con una opción para automatizar las acciones de respuesta durante todo el día.

Supere su habilidad o falta de recursos respondiendo a los ataques con un proveedor de servicios certificado respaldado por F-Secure

SENSORES DE PUNTO FINAL

Herramientas de monitoreo ligeras y discretas diseñadas para funcionar con cualquier solución de protección de punto final.

Los sensores ligeros se implementan en todas las computadoras relevantes dentro de su organización.

Los sensores recopilan datos de comportamiento de los puntos finales de Windows y Mac.

Específicamente diseñado para soportar ataques de varios adversarios.

RESPUESTA GUIADA

Te prepara para enfrentar incluso los ataques cibernéticos más avanzados con tus recursos existentes.

Proveedores certificados y capaces lo guían a través de diferentes escenarios de incumplimiento.

Acciones de respuesta con orientación paso a paso, soporte adicional y asesoramiento.

Los proveedores de servicios gestionados siempre están capacitados y respaldados por F-secure.

DETECCIÓN DE CONTEXTO AMPLIO

Entender el alcance de un ataque dirigido es fácil..

Análisis de comportamiento, reputación y big data en tiempo real con aprendizaje automático.

Coloca automáticamente las detecciones en un contexto visualizado en una línea de tiempo.

Incluye los niveles de riesgo, la criticidad del huésped afectado y el panorama de amenazas prevaleciente.

RESPUESTA AUTOMATIZADA

Reduzca el impacto de los ataques cibernéticos dirigidos al contener amenazas durante todo el día.

Acciones de respuesta automatizadas basadas en criticidad, niveles de riesgo y un calendario predefinido.

La crítica y los niveles de riesgo proporcionados por la solución también mejoran la priorización de las acciones de respuesta.

Permite a los equipos que solo están disponibles durante el horario comercial contener ataques rápidamente

APLICACIÓN VISIBILIDAD

Ganar visibilidad en su entorno de TI y estado de seguridad nunca ha sido tan fácil

Identifica todas las aplicaciones no deseadas o no deseadas, y los destinos extranjeros de diferentes servicios en la nube.

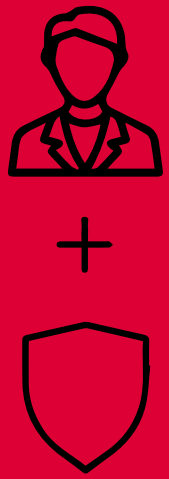
Aprovecha los datos de reputación de F-Secure para identificar aplicaciones potencialmente dañinas.

Restringe aplicaciones potencialmente dañinas y servicios en la nube incluso antes de que ocurran violaciones de datos.

PARA UN VIDEO VE:

www.f-secure.com/EDR

HOMBRE + MÁQUINA



¿Cómo detectas un ataque sofisticado? Usted hace uso de las tecnologías más avanzadas de análisis y aprendizaje automático. Pero eso no es todo. Tienes que pensar como un atacante.

Los expertos en seguridad de F-secure han participado en más investigaciones de delitos cibernéticos en Europa que ninguna otra empresa. Con los dedos de nuestros expertos firmemente en el pulso del panorama del ataque cibernético, se mantendrá al día con la última información sobre amenazas.

Nadie conoce la seguridad cibernética como F-Secure. Durante tres décadas, F-secure ha impulsado innovaciones en seguridad cibernética, defendiendo a decenas de miles de empresas y millones de personas. Con una experiencia insuperable en la protección de puntos finales, así como en la detección y respuesta, F-secure protege a empresas y consumidores contra todo, desde ataques cibernéticos avanzados y violaciones de datos hasta infecciones de ransomware generalizadas.

La sofisticada tecnología de F-Secure combina el poder del aprendizaje automático con la experiencia humana de sus laboratorios de seguridad de renombre mundial para un enfoque singular llamado Live Security. Los expertos en seguridad de F-Secure han participado en más investigaciones europeas sobre la escena del crimen cibernético que cualquier otra compañía en el mercado, y sus productos se venden en todo el mundo a través de más de 200 operadores de banda ancha y móviles y miles de revendedores. Fundada en 1988, F-Secure cotiza en NASDAQ OMX Helsinki Ltd.

www.f-secure.com
www.twitter.com/fsecure
www.facebook.com/f-secure

F-Secure