CROWDSTRIKE

DETECCIÓN Y RESPUESTA PARA ENDPOINTS (EDR) DE LA PLATAFORMA FALCON

Transmitiendo el ciclo de vida de la respuesta y detección de amenazas con velocidad, automatización y visibilidad inigualables

FALCON INSIGHT — EDR FÁCIL

Las herramientas tradicionales de seguridad de endpoints tienen puntos ciegos, lo que les impide ver y detener las amenazas avanzadas. CrowdStrike® Falcon Insight™ resuelve esto ofreciendo visibilidad completa sobre los endpoints en toda su organización.

Falcon Insight monitorea continuamente toda la actividad de los endpoints y analiza los datos en tiempo real para identificar automáticamente actividades de amenaza, lo que le permite detectar y prevenir amenazas avanzadas a medida que éstas ocurren. Toda la actividad de los endpoints también se transmite a la plataforma CrowdStrike Falcon® para que los equipos de seguridad puedan, rápidamente, investigar incidentes, responder a alertas y cazar nuevas amenazas de forma proactiva.

CROWDSTRIKE ES RECONOCIDA CONSTANTEMENTE COMO UNA SOLUCIÓN LÍDER EN PROTECCIÓN DE ENDPOINTS

CrowdStrike está posicionada como líder en el Cuadrante Mágico de Gartner de 2019 para Plataformas de Protección de Endpoints

CrowdStrike está validada por las Pruebas de Emulación MITRE de Estado- nación 2018 contra el marco MITRE ATT&CK™ para rastrear y detectar ataques avanzados

CrowdStrike es el único proveedor posicionado como líder en el Forrester Wave™: Respuesta y Detección para Endpoints, tercer trimestre de 2018, así como en el Forrester Wave: Paquetes de Seguridad para Endpoints, tercer trimestre de 2019

CrowdStrike obtuvo la mejor calificación entre las organizaciones "Tipo A" en Capacidades Críticas de Plataformas de Protección de Endpoints de octubre de 2019 de Gartner

PRINCIPALES BENEFICIOS

Detecte y priorice las amenazas avanzadas de forma automática e inteligente

Acelere las investigaciones con análisis forenses detallados y en tiempo real y visualizaciones sofisticadas

Responda y remedie con confianza

Obtenga una visión integral con CrowdScore™, su calificación de amenazas empresariales

Reduzca la fatiga de alertas en un 90% o más

Comprenda los ataques de mayor complejidad en tan solo un vistazo con el marco de detección basado en MITRE y el CrowdScore Incident Workbench

DETECCIÓN Y RESPUESTA PARA ENDPOINTS (EDR) DE LA PLATAFORMA FALCON

PRINCIPALES CAPACIDADES DEL PRODUCTO

SIMPLIFIQUE LA DETECCIÓN Y SOLUCIÓN

- **Detecte automáticamente las actividades del atacante:** Falcon Insight utiliza IOAs (indicadores de ataque) para identificar automáticamente el comportamiento del atacante y enviar alertas priorizadas a la interfaz de usuario (UI, por sus siglas en inglés) de la plataforma Falcon, eliminando investigaciones y búsquedas manuales que consumen mucho tiempo. La base de datos de la Threat Graph® de CrowdStrike almacena información de eventos y responde consultas en cinco segundos o menos, incluso cuando se trata de miles de millones de eventos.
- **Despliegue ataques enteros en tan solo una pantalla:** El CrowdScore Incident Workbench ofrece una visión completa de un ataque, desde el inicio hasta el final, con un contexto detallado para investigaciones más rápidas y fáciles.
- **Acelere el flujo de trabajo de las investigaciones con MITRE ATT&CK™:** Esquematizar las alertas con el marco de Tácticas, Técnicas y Conocimientos Comunes (ATT&CK™) de MITRE le permite comprender hasta las detecciones más complejas en tan solo un vistazo, reduciendo el tiempo necesario para la clasificación de alertas y acelerando la priorización y remediación. Además, la UI intuitiva le permite pivotar rápidamente y buscar en toda su organización en cuestión de segundos.
- **Obtenga contexto e inteligencia:** la inteligencia integrada de amenazas provee el contexto completo de un ataque, incluyendo su atribución.
- **Responda de manera decisiva:** Actúe contra los adversarios en tiempo real para detener los ataques antes de que se conviertan en brechas. Las potentes acciones de respuesta le permiten contener e investigar sistemas comprometidos. Las Capacidades de Respuesta en Tiempo Real del Falcon Insight proveen acceso directo a los endpoints bajo investigación. Esto les permite a los respondedores de seguridad ejecutar acciones en el sistema y erradicar amenazas con extrema precisión.

OBTENGA VISIBILIDAD DEL ESPECTRO COMPLETO EN TIEMPO REAL

- **Vea el panorama general en tiempo real:** CrowdScore ofrece una métrica simple que le ayuda a una organización a comprender su nivel de amenaza en tiempo real. Esto les permite a los líderes de seguridad comprender rápidamente si están siendo atacados y evaluar la gravedad de la amenaza para coordinar la respuesta adecuada.
- **Capture detalles importantes para la cacería de amenazas y las investigaciones forenses:** el controlador en modo kernel del Falcon Insight captura más de 400 eventos sin procesar, así como la información relacionada que se requiere para volver a rastrear incidentes.
- **Obtenga respuestas en segundos:** La base de datos de la Threat Graph® de CrowdStrike almacena información de eventos y responde consultas en cinco segundos o menos, incluso cuando se trata de miles de millones de eventos.
- **Recupere información de hasta 90 días:** el Falcon Insight provee un registro completo de la actividad de los endpoints en el tiempo, independientemente de si su entorno está compuesto por menos de 100 endpoints o más de 500.000.

RELACIÓN VALOR-TIEMPO INMEDIATA

- **Ahorre tiempo, esfuerzo y dinero:** Falcon Insight, habilitado en la nube por la plataforma CrowdStrike Falcon, no requiere ninguna infraestructura de administración on-premise.
- **Implementación en segundos:** los clientes de CrowdStrike pueden implementar el agente Falcon en la nube en hasta 70,000 endpoints en menos de un día.
- **Entra en operación de manera inmediata:** Con una detección y visibilidad inigualables desde el primer día, el Falcon Insight comienza a funcionar, monitorear y registrar rápidamente tras su instalación, sin necesidad de reinicios, ajustes específicos, líneas base o configuraciones complejas.
- **Cero impacto en el endpoint:** con apenas un agente liviano en el endpoint, las búsquedas se realizan en la base de datos de la Threat Graph, sin ningún impacto en el desempeño de los endpoints o de la red.

Más información en www.crowdstrike.com

SOBRE CROWDSTRIKE

CrowdStrike® Inc (Nasdaq: CRWD)., un líder mundial en ciberseguridad, está redefiniendo la seguridad en la era de la nube con una plataforma de protección de endpoints construida desde cero para detener las brechas. La arquitectura de un agente único y liviano de la plataforma CrowdStrike Falcon® aprovecha la inteligencia artificial (IA) a escala de nube y ofrece protección y visibilidad en tiempo real en toda la empresa, previniendo ataques en endpoints, dentro o fuera de la red. Con la tecnología patentada de la CrowdStrike Threat Graph®, CrowdStrike Falcon correlaciona más de tres billones de eventos por semana, y en tiempo real, relativos a endpoints de todo el mundo, alimentando una de las plataformas de datos más avanzadas del mundo en seguridad.

DESCARGO DE RESPONSABILIDAD:

Gartner no respalda ningún proveedor, producto o servicio descrito en sus publicaciones de investigaciones, y no les aconseja a los usuarios de tecnología que seleccionen solo aquellos proveedores con las calificaciones más altas. Las publicaciones de investigación de Gartner consisten en opiniones de la organización de investigación de Gartner y no deben interpretarse como declaraciones de hecho. Gartner niega todas las garantías, expresas o implícitas, con respecto a esta investigación, incluidas las garantías de comerciabilidad o idoneidad para un propósito particular.