CROWDSTRIKE

Cinco capacidades fundamentales para protegerse del riesgo de los endpoints

Intensifica la detección y la respuesta en toda tu empresa

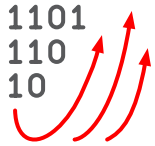
eBook de CrowdStrike

Índice

Los defensores se merecen más

Hasta 2020, los equipos de TI y de seguridad tenían serias dificultades para gestionar y proteger los endpoints. Muchas empresas se las apañaban con soluciones para endpoints que actuaban como herramientas básicas de administración de dispositivos. Hoy día, gracias a la protección de endpoints moderna, incluso dadas las necesidades de gestionar equipos de trabajo remotos e híbridos, operacionalizar las iniciativas de transformación digital y desenvolverse en un panorama de amenazas volátiles, hay visos de mejora.

La protección de los endpoints es uno de los problemas de seguridad más importantes para los entornos de trabajo modernos.



Aumenta el número de endpoints que acceden a aplicaciones, infraestructuras y datos en la nube.

El empleo de distintos productos independientes y soluciones de seguridad tradicionales no proporciona una visibilidad total.

Los ciberdelincuentes son implacables y aprovechan la complejidad para lanzar ataques más rápidos y sofisticados.

La protección de endpoints actual debe hacer frente a atacantes que cuentan con todos los recursos.

El acceso a las credenciales es más fácil ahora; los intermediarios de acceso aumentaron el volumen de anuncios un

112 % en 2022

respecto a 2021.

El tiempo de propagación ha descendido hasta los

84 minutos

Una empresa media utiliza

45 herramientas de seguridad diferentes

Fuente: Global Threat Report 2023 de CrowdStrike

El nuevo mundo de la protección moderna de los endpoints

La complejidad del panorama de las amenazas, junto con el empleo de soluciones tradicionales para endpoints crean obstáculos infranqueables para los equipos de TI y de seguridad. Los defensores se topan a diario con dificultades como la inflexibilidad operativa, las actividades manuales (como el análisis de los registros) y la detección de ataques a posteriori.

Las plataformas de protección de endpoints han sido diseñadas para corregir estos problemas y mejorar el flujo de trabajo de los analistas, priorizando la resiliencia contra las amenazas.

Ha llegado el momento de que los defensores se sientan capacitados para abordar las amenazas de ciberseguridad más urgentes.

La protección de endpoints moderna ayuda a tu empresa a:

- ✓ Conseguir mejores resultados
- ✓ Maximizar la seguridad, y el valor operativo y económico

CINCO CAPACIDADES CLAVE

1	2	3	4	5
PREVENCIÓN	**DETECCIÓN**	**THREAT HUNTING GESTIONADO**	**INTELIGENCIA SOBRE AMENAZAS**	**GESTIÓN DE VULNERABILIDADES E HIGIENE DE TI**
Antivirus de nueva generación (NGAV)	Detección y respuesta para endpoints (EDR)	Equipos humanos de Threat Hunting proactivo	Anticipación	Preparación

En este eBook, revelamos cómo puedes agregar valor a tu equipo de seguridad, sin agotar tus recursos. Continúa leyendo para conocer mejor cada uno de estos elementos clave de los endpoints.

Prevención: cerrar el paso a los ciberdelincuentes

La protección de endpoints tradicional centrada en el malware —como las soluciones antivirus— suele ser eficaz únicamente frente al malware conocido. Dado que ahora los ciberdelincuentes optan por utilizar tácticas más sofisticadas sin archivos ni malware, para muchas empresas ha llegado el momento de modernizar su protección.

Los equipos de TI y de seguridad necesitan la inteligencia de una solución antivirus de nueva generación (NGAV) que sea capaz de reconocer y prevenir:

- El malware conocido y de día cero
- El ransomware
- Los ataques fileless y sin malware

Gracias a una combinación de inteligencia artificial, detección de comportamientos, algoritmos de Machine Learning (ML) y mitigación de exploits, las soluciones NGAV avanzadas prevén y evitan inmediatamente las amenazas conocidas y desconocidas.

A diferencia de las soluciones tradicionales, que requieren actualizaciones diarias, las soluciones NGAV utilizan ML para mantener la seguridad al día, liberando el tiempo empleado en estas tediosas tareas.

Las soluciones NGAV avanzadas combinan técnicas que proporcionan la visibilidad y el contexto necesarios para impedir que las tácticas, técnicas y procedimientos (TTP) de ataque modernos logren su objetivo.

La actividad sin el uso de malware va en aumento

71 %	**2022**
62 %	2021
51 %	2020
40 %	2019
39 %	2018

Fuente: Global Threat Report 2023 de CrowdStrike

¿Por qué se está dejando de usar el malware?

- Generalización del uso ilícito de credenciales válidas para facilitar el acceso y la persistencia en los entornos de las víctimas
- Las nuevas vulnerabilidades se divulgan más rápidamente y los ciberdelincuentes ponen práctica los exploits a más velocidad

Detección: encontrar y eliminar a los atacantes que se infiltran

Ni la mejor estrategia de prevención consigue frenar a los atacantes actuales sofisticados y bien financiados. Lo más seguro es integrar la prevención con una eficaz estrategia de detección para poder identificar y responder rápidamente a los ataques furtivos más complejos.

Sobrevive el más rápido

CrowdStrike registra un parámetro denominado "tiempo de propagación" que indica cuánto tarda un atacante en moverse lateralmente desde el host que comprometió inicialmente hasta otro dentro del entorno de la víctima. El tiempo de propagación medio para una intrusión ciberdelictiva interactiva descendió de 98 minutos en 2021 a solo 84 minutos en 2022. Detectar y responder dentro del plazo de propagación ofrece a los defensores más posibilidades de minimizar los costes, así como otros daños provocados por el atacante.

Según los profesionales de la seguridad, el empleo de herramientas descoordinadas, plataformas aisladas y consolas independientes facilita a los ciberdelincuentes el acceso inicial sin hacer sonar las alarmas.Los conjuntos de soluciones de seguridad cada vez son más complejos y esto permite a los atacantes aprovechar los vacíos de visibilidad y prolongar su permanencia.

Una seguridad de endpoints moderna debe proporcionar visibilidad, detección y respuesta globales, en todo el parque de endpoints, en cualquier lugar del mundo. La plataforma CrowdStrike Falcon® unificada proporciona a los equipos de seguridad sencillas funciones de detección y respuesta extendidas (XDR) de categoría empresarial, basadas en un sistema líder de detección y respuesta para endpoints (EDR).

Con esta estrategia de detección, incluso si un ciberdelincuente consigue infiltrarse en un sistema, la función de EDR señala claramente sus intentos de movimiento lateral y acceso a otros sistemas y:

- Registra todas las actividades que merezcan una inspección más detallada en tiempo real y tras la actividad
- Muestra el comportamiento sospechoso, desde el inicio hasta la finalización
- Enriquece los datos con inteligencia sobre amenazas relacionada con el adversario para proporcionar el contexto necesario para llevar a cabo con éxito los procesos de Threat Hunting y clasificación
- Facilita una respuesta rápida, completa y remota en múltiples endpoints

84 minutos es el tiempo que necesita un atacante para moverse lateralmente. Se denomina **tiempo de propagación** e indica cuánto tarda un ciberdelincuente en avanzar desde el host que comprometió inicialmente hasta otro host dentro del entorno de la víctima.

Fuente: Global Threat Report 2023 de CrowdStrike

Threat Hunting gestionado: llevar la detección más allá de las defensas automatizadas

Una estrategia proactiva ejecutada por humanos para buscar de manera activa acciones sospechosas ofrece el equilibrio perfecto entre el empleo de tecnología y de expertos. En lugar de depender exclusivamente de la tecnología para detectar y alertar automáticamente de posibles actividades de ataque, los Threat Hunters pueden anticiparse a las ciberamenazas contra la empresa.

A menudo no es posible contar con un equipo interno de expertos para monitorizar permanentemente el entorno y detectar las actividades maliciosas. El Threat Hunting gestionado da respuesta a estas necesidades de personal especializado.

Los Threat Hunters adoptan un enfoque proactivo en cuanto a la protección de endpoints. Gracias a sus años de experiencia, ofrecen a las empresas una remediación completa sin necesidad de ampliar su personal. La visibilidad del estado de los endpoints y el acceso a la inteligencia adecuada sobre amenazas les permiten entender lo que observan y anticiparse a las ciberamenazas contra la empresa para mitigar el riesgo.

Escasez mundial de expertos en ciberseguridad

3,4 millones de personas

Fuente: (ISC)² 2022 Cybersecurity Workforce Study

Los equipos de Threat Hunting gestionado analizan las amenazas y trabajan codo con codo con el personal interno para guiarle desde la detección hasta la respuesta. Esta interacción con expertos mejora el nivel de madurez de los equipos de seguridad y TI internos, no solo en ese preciso momento, sino también a la larga.

Inteligencia sobre amenazas: conocer y prever los ataques

Para las empresas es fundamental conocer y predecir los ataques avanzados gracias a la inteligencia de amenazas, para poder detenerlos. Para reforzar tu SOC, las soluciones de seguridad de endpoints deben incorporar inteligencia sobre amenazas que no se limite a la obtenida de fuentes públicas, poco fiable y generada a posteriori.

La inteligencia sobre amenazas debe cumplir los siguiente requisitos:

- **Proporcionar información práctica** que permita a los equipos de seguridad y a las soluciones que utilizan comprender, responder y resolver los incidentes de manera más rápida, agilizando las investigaciones y la remediación.
- **Generar y priorizar alertas** que ayuden a los equipos de seguridad a conocer mejor las tácticas y las campañas asociadas a determinados ciberdelincuentes.
- **Estar integrada a la perfección en la solución de protección de endpoints** de modo que esté al alcance de los equipos de seguridad y TI. Además, si se proporciona en una sola consola, los analistas pueden ver el contexto de una alerta y descubrir los detalles con solo hacer clic.

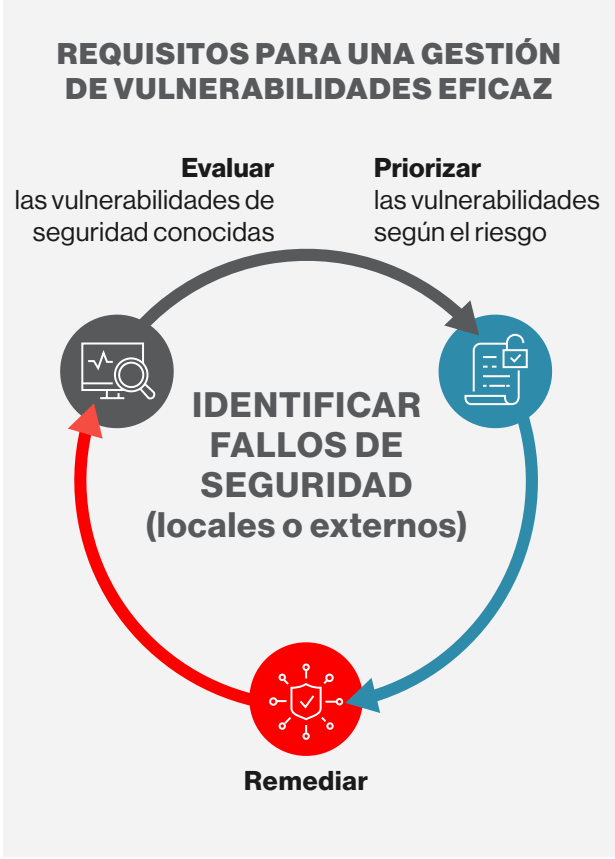
La inteligencia sobre amenazas debe estar integrada en el flujo de trabajo del SOC, debe estar correlacionada con los últimos datos sobre vulnerabilidades y, lo que es más importante, debe contar con la confianza de todo el equipo de seguridad para proporcionar continuamente información de amenazas puntual, precisa y relevante.

Gestión de vulnerabilidades e higiene de TI: blindar el entorno frente ataques

Los equipos de TI y seguridad deben saber qué sistemas y aplicaciones están en riesgo, así como quién y qué hay activo en el entorno. La gestión de vulnerabilidades y la higiene de TI ofrecen la visibilidad y la información práctica necesarias para conseguirlo.

A pesar de sus esfuerzos, inevitablemente, dado el constante aumento de las vulnerabilidades críticas, a las empresas les faltarán algunos parches y mitigaciones. Dedicar a cada vulnerabilidad el tiempo necesario para mitigarla y responder para proteger el entorno es una tarea ingente, cuando no imposible.

Las amenazas activadas por humanos son la principal causa de las brechas actuales. Las soluciones de higiene de TI ofrecen visibilidad de las tendencias de inicio de sesión (las actividades y su duración) en todo el entorno, dondequiera que se utilicen credenciales existentes o se creen nuevas credenciales de administrador. Al tener acceso a todos los detalles, los equipos de seguridad pueden detectar y mitigar con confianza el uso indebido de credenciales y los ataques basados en credenciales robadas.



88 %

de todas las brechas de datos son provocadas por el error de un empleado

Fuente: Stanford, Psychology of Human Error

Las soluciones de higiene de TI monitorizan continuamente posibles cambios en los recursos, las aplicaciones y los usuarios. Esto ayuda a identificar los sistemas no gestionados o los que pueden comportar un riesgo para la red, como los dispositivos de terceros o personales (BYOD) no protegidos.

Da el paso siguiente

El tiempo de propagación de los ataques ha descendido y las tecnologías de ML e IA son cada vez más fáciles de utilizar, por lo que es evidente que los ciberdelincuentes aumentarán el ritmo de ataque. Tu empresa necesita una solución de seguridad de endpoints que utilice estas circunstancias a su favor.

Mejora la tecnología y los expertos, para comenzar. Aumenta la protección, para terminar.

Las cinco capacidades descritas en este eBook te proporcionarán el nivel detallado de visibilidad y control que necesitas para vencer al adversario. Sin embargo, los productos independientes para cada funcionalidad no ofrecen el grado de velocidad, flexibilidad y capacidad necesario para defenderse de los ataques actuales.

Las empresas deben adoptar una solución totalmente habilitada e integrada, proporcionada a través de una plataforma nativa en la nube, como CrowdStrike Falcon. Con detecciones hiperprecisas, protección y remediación automatizadas, Threat Hunting de élite y observabilidad de vulnerabilidades por prioridades, la solución líder del sector de CrowdStrike puede proteger a todas las empresas, desde las pequeñas hasta las corporaciones internacionales.

Erradica las amenazas con protección para varios dominios y varios proveedores, sin interrupciones de la actividad empresarial y maximizando la rentabilidad de la inversión.

Compartir

Comparte este eBook en tus canales sociales para difundir la importancia de la protección contra riesgos en los endpoints.

Tuitear | Compartir | Compartir

Participar

Consigue protección rápida y sencilla para todas las amenazas con nuestra prueba gratuita. Una plataforma nativa en la nube, que se despliega totalmente en minutos.

Probar

Conectar

Reserva con nuestra sencilla herramienta de planificación una reunión con CrowdStrike para obtener más información. Selecciona la hora que prefieras.

Planificar

Acerca de CrowdStrike

CrowdStrike (Nasdaq: CRWD), líder mundial en ciberseguridad, ha redefinido la seguridad moderna con la plataforma nativa en la nube más avanzada del mundo, para proteger aspectos fundamentales del riesgo empresarial: las cargas de trabajo, la identidad y los datos, tanto en los endpoints como en la nube.

Gracias a CrowdStrike Security Cloud y una inteligencia artificial de talla mundial, la plataforma CrowdStrike Falcon® se nutre de indicadores en tiempo real, inteligencia sobre amenazas, información de las herramientas evolutivas de los adversarios y telemetría enriquecida con datos de toda la empresa, para facilitar detecciones hiperprecisas, protección y remediación automatizadas, Threat Hunting de élite y observación de vulnerabilidades por prioridades.

Desarrollada expresamente en la nube con una arquitectura de agente ligero único, la plataforma Falcon ofrece un despliegue rápido y escalable, protección y rendimiento superiores, menor complejidad y rentabilidad inmediata.

CrowdStrike: We stop breaches.

Más información

Síguenos:

- **Blog ›**
- **Twitter ›**
- **LinkedIn ›**
- **Facebook ›**
- **Instagram ›**

Empieza una prueba gratuita hoy mismo

CROWDSTRIKE