CROWDSTRIKE

Los ciberdelincuentes y las técnicas de evasión actuales: por qué los antivirus tradicionales son un objetivo fácil

eBook de CrowdStrike

Índice

Por qué fallaron los antivirus tradicionales

Si hubiera que extraer una sola idea de este eBook, sería esta: los antivirus (AV) tradicionales ya no frenan a los ciberdelincuentes. Para evitar las brechas se necesita una seguridad de endpoints moderna, y punto.

¿En qué fallaron los antivirus tradicionales? En primer lugar, se trata de una tecnología que tiene décadas y es muy lenta; su implementación lleva meses; y los interminables análisis y actualizaciones que requiere consumen los recursos y ralentizan el funcionamiento de los endpoints. En otras palabras, mientras que los atacantes cada vez son más rápidos, los antivirus tradicionales son cada vez más lentos.

Pero el principal problema es que básicamente ya no funcionan. La tecnología se basa exclusivamente en firmas, que son difíciles de actualizar y no son eficaces contra los ataques fileless. Ahora que el 71 % de los casos detectados no incluyen malware,[1] para una tecnología que depende exclusivamente de las amenazas conocidas, la mayoría de los ataques pasan desapercibidos.

Estos defectos no implican que se haya invertido poco esfuerzo. Algunos proveedores de antivirus tradicionales han añadido en los últimos años análisis de comportamientos y Machine Learning (ML). Sin embargo, el resultado es una amalgama de agentes adicionales que resulta complicada de desplegar y gestionar. Los nuevos agentes con frecuencia carecen de integración nativa con los agentes existentes, lo que obliga a los clientes a configurar conexiones entre ellos. Para cuando se consigue desplegar un nuevo agente, ya ha quedado obsoleto.

Sigue leyendo para descubrir cómo consiguen los ciberdelincuentes sortear la protección de los antivirus tradicionales, conocer cinco ilustrativos casos de ciberdelincuentes en acción y entender por qué la seguridad de endpoints moderna es la única forma de detener las brechas. Comencemos.

71 %

de los ataques detectados no incluyen malware

=

560 000

nuevas muestras de malware detectadas al día

Cómo sortean los ciberdelincuentes la defensa de los antivirus tradicionales

Hasta hace poco tiempo, el malware era el punto de acceso preferido entre los ciberdelincuentes, sin embargo, esto ha cambiado. Si bien el malware sigue constituyendo una amenaza importante —con 560 000 nuevos ejemplares de malware detectados cada día y más de mil millones de programas de malware disponibles en circulación[2]—, según la investigación de CrowdStrike, el malware se usa ahora más adelante en la cadena de ataque.

Veamos siete nuevas técnicas de evasión de las defensas, **según MITRE**.

[1] Global Threat Report 2023 de CrowdStrike
[2] DataProt. A Not-So-Common Cold: Malware Statistics in 2023. Marzo de 2023.

Siete técnicas para evadir la defensa que los antivirus tradicionales no consiguen evitar

1. Dañar las defensas: los ciberdelincuentes pueden modificar componentes del entorno de una víctima para obstaculizar o inhabilitar los mecanismos de defensa, como las medidas de protección preventivas (firewalls y antivirus) o las funciones de detección utilizadas para auditar la actividad e identificar comportamientos maliciosos.

2. Borrar indicios: los atacantes pueden eliminar o modificar artefactos generados en los sistemas con el fin de borrar pruebas de su presencia o dificultar el trabajo de las defensas. Un ciberdelincuente, o sus acciones, pueden dar lugar a distintos artefactos, como la eliminación u ocultación de archivos.

3. Alterar los controles de confianza: otro método que emplean los ciberdelincuentes para sortear la protección de los antivirus tradicionales es debilitar los controles de confianza que avisan a los usuarios de una actividad no fiable o bien impiden la ejecución de programas no seguros. Los sistemas operativos y los productos de seguridad pueden contener mecanismos para identificar si los programas o sitios web tienen algún nivel de confianza. Los ciberdelincuentes pueden intentar dañar estos mecanismos para modificar registros o permisos para archivos y directorios. Además, pueden crear o robar certificados de firma de código para que se les considere de confianza en los sistemas atacados.

4. Secuestrar el flujo de ejecución: los atacantes pueden ejecutar sus propias payloads maliciosas secuestrando el proceso de ejecución de los programas en el sistema operativo. Esto puede ofrecerles persistencia, ya que el proceso secuestrado puede repetirse en el futuro. Además, los atacantes podrían usar también estos mecanismos para elevar los privilegios o bien sortear defensas como el control de aplicaciones.

5. Inyectar código en los procesos: esto permite a los atacantes evadir las defensas basadas en procesos o elevar los privilegios. La inyección en los procesos es un método de ejecución de código arbitrario en el espacio de direcciones de un proceso activo diferente. Ejecutar el código en el contexto de otro proceso puede facilitar el acceso a la memoria del proceso y/o a los recursos del sistema o la red, y posiblemente permitir una elevación de privilegios.

6. Ejecutar contenido a través de un binario proxy del sistema: los atacantes pueden sortear las defensas basadas en firmas y/o procesos ejecutando contenido malicioso a través de un archivo binario firmado (proxy) o que cuente con algún otro tipo de confianza. Los binarios que se emplean para esta técnica suelen ser archivos firmados de Microsoft, lo que indica que se han descargado de Microsoft o bien ya son nativos del sistema operativo.

7. Ocultarse: otro método que emplean los atacantes para sortear la protección de los antivirus tradicionales es manipular las características de sus artefactos de manera que parezcan legítimos o lícitos ante los usuarios y/o las herramientas de seguridad. La ocultación se produce mediante la manipulación o alteración del nombre o la ubicación de un objeto —legítimo o malicioso— para evadir las defensas y evitar ser detectado. Para ello, se pueden manipular metadatos de archivos, confundir a los usuarios para que no identifiquen el tipo de archivo y utilizar nombres de tareas o servicios legítimos.

Según las investigaciones de CrowdStrike,

86 %

de los ciberdelincuentes emplean una o varias técnicas de evasión para escapar al tipo de detección que ofrece el software antivirus tradicional.

Desde los antivirus tradicionales hasta la seguridad de endpoints moderna

La seguridad de endpoints moderna es una estrategia de protección integral diseñada para detectar las técnicas de evasión de las defensas y, en última instancia, frenar las brechas de seguridad. A un nivel básico, incluye dos componentes: un antivirus de nueva generación (NGAV) y una solución de detección y respuesta para endpoints (EDR).

¿Qué es un NGAV?

Un NGAV es una herramienta de ciberseguridad que usa una combinación de inteligencia artificial, detección de comportamientos, algoritmos de Machine Learning y mitigación de exploits, para adelantarse y prevenir todo tipo de amenazas, ya sean conocidas o desconocidas. A diferencia de las soluciones antivirus tradicionales, las de nueva generación, o NGAV, se basan en la nube, lo que permite desplegarlas más rápidamente y sin sobrecargar el endpoint. Además, eliminan o reducen significativamente el trabajo de mantenimiento del software, administración de la infraestructura y actualización de las bases de datos de firmas.

¿Qué es EDR?

EDR es una solución de ciberseguridad que detecta y mitiga las amenazas, mediante la supervisión continua de los dispositivos endpoint y el análisis de sus datos. Las soluciones EDR proporcionan en tiempo real visibilidad continua y global de lo que ocurre en todos los endpoints. A continuación, aplican análisis de comportamientos e inteligencia práctica a los datos de los endpoints para evitar que un incidente pueda convertirse en una brecha. Además, las herramientas EDR proporcionan funciones avanzadas de detección de amenazas, investigación y respuesta, que incluyen la búsqueda de datos de incidentes y su investigación, la clasificación de alertas, la comprobación de actividad sospechosa, Threat Hunting, y la detección y contención de actividades maliciosas.

Dado que los ciberdelincuentes son cada vez más sofisticados y sus tácticas, técnicas y procedimientos (TTP) evolucionan constantemente, las empresas deben usar tanto soluciones EDR como NGAV para disfrutar de una protección total contra los ataques modernos.

A continuación, descubre cinco reveladores casos de ciberdelincuentes que consiguieron evadir el antivirus tradicional y cómo la seguridad de endpoints moderna habría frenado las brechas.

Cinco técnicas de evasión de la protección en acción

Atacante:

WANDERING SPIDER

Cuándo
A principios de 2023

Qué ocurrió
CrowdStrike Intelligence llevaba siguiendo el rastro de WANDERING SPIDER desde abril de 2020. Este ciberdelincuente ha ejecutado campañas de ransomware mediante Black Basta, DoppelPaymer de DOPPEL SPIDER, REvil y ProLock de PINCHY SPIDER, Egregor y Maze de TWISTER SPIDER, y Conti de WIZARD SPIDER. A principios de 2023, CrowdStrike descubrió que WANDERING SPIDER estaba usando el binario legítimo `fs _ uninstall _ 32.exe` para desinstalar una solución antivirus tradicional para empresas.

Cómo ayuda la seguridad de endpoints moderna
Una forma que tienen los ciberdelincuentes de escapar a la detección es utilizar herramientas legítimas para mezclarse entre las actividades cotidianas lícitas. Estos tipos de ataques son extremadamente difíciles de detectar con métodos basados en firmas. Sin embargo, la seguridad de endpoints moderna da un resultado excelente, ya que permite distinguir los comportamientos maliciosos de los lícitos. Por ejemplo, las funciones contra falsificación bloquean los intentos de manipulación con el sensor. De esta forma, protegen los archivos, carpetas y objetos del registro relacionados con el sensor, para evitar que se cambie su nombre o se eliminen. Aunque se desactive, el sensor identifica y alerta sobre los intentos de falsificación.

Atacante:

MALLARD SPIDER

Cuándo
Febrero de 2023

Qué ocurrió
Fuentes del sector denunciaron una campaña de spam por correo electrónico que distribuía QakBot usando archivos WSF de Windows que se hacían pasar por un certificado. El archivo WSF contenía código JavaScript incrustado que intentaba descargar y ejecutar la payload QakBot. Tras el declive de los métodos de distribución que emplean ISO y OneNote, los ciberdelincuentes han estado probando otras alternativas y tácticas de ocultación, incluidas algunas que ya se habían observado antes, como el contrabando de HTML, archivos ZIP protegidos con contraseña, codificación Base64 y exageración del tamaño de archivos. Estas técnicas suelen ser eficaces para superar los análisis de los antivirus tradicionales.

Cómo ayuda la seguridad de endpoints moderna
Los atacantes continúan probando nuevas formas de distribución de malware y emplean tácticas como ocultar caracteres y la codificación Base64 para escapar a las detecciones basadas en firmas. La seguridad de endpoints moderna, gracias al uso de indicadores de compromiso, IA avanzada y análisis de comportamientos, ofrece una detección temprana de las técnicas de ocultación y los intentos de ejecución de payloads maliciosas, lo que permite detener estos ataques.

Atacante:

SCATTERED SPIDER

Cuándo
A principios de 2023

Qué ocurrió
CrowdStrike Intelligence detectó actividad potencial de **SCATTERED SPIDER** en la que el atacante accedía a varias empresas tecnológicas de América del Norte especializadas en externalización de procesos empresariales. Aunque no se llegaron a confirmar los vectores de infección, el atacante desplegó herramientas de administración y supervisión remotas (RMM) o probó la capacidad para acceder a dominios relacionados con este tipo de software. Además, SCATTERED SPIDER utilizó numerosas utilidades de tipo "living-off-the-land" (LotL) y herramientas legítimas para llevar a cabo parte de su actividad posterior al exploit. Normalmente, los proveedores de antivirus tradicionales no consiguen analizar las herramientas RMM y legítimas, por lo que no pueden impedir este tipo de ataques contra la cadena de suministro.

Cómo ayuda la seguridad de endpoints moderna
La seguridad de endpoints moderna emplea análisis avanzados de comportamientos para conocer el contexto de la actividad aparentemente legítima. En este caso, el atacante accedió a un sitio web legítimo, aunque poco utilizado, y procedió a iniciar sesión en los sistemas de las víctimas para ejecutar comandos de reconocimiento, como `mmc.ex` para obtener información del Directorio Activo o `whoami` para hallar la cuenta del usuario que tenía iniciada una sesión. Una solución de seguridad de endpoints moderna habría detectado y detenido esta actividad maliciosa.

Atacante:

Raccoon Stealer Customer

Cuándo
Agosto de 2022

Qué ocurrió
CrowdStrike Intelligence identificó una nueva campaña de phishing con un cargador basado en .NET muy oculto que intentaba descargar e instalar una muestra del nuevo Raccoon Stealer 2.0. El popularísimo Raccoon Stealer es un diminuto paquete de malware que puede incluirse fácilmente en paquetes de mayor tamaño. Habitualmente, cuando los usuarios descargan un paquete grande, los proveedores de antivirus tradicionales no analizan todos sus componentes, lo que permite al malware colarse de manera inadvertida.

Cómo ayuda la seguridad de endpoints moderna
Esta detección se realizó observando un downloader que utiliza varias técnicas de evasión para escapar a la detección a nivel de host y de red, como payloads fileless de varias fases, distintos tipos de ocultaciones y herramientas legítimas, como Discord y OneDrive, para alojar las fases posteriores. La seguridad de endpoints moderna, que combina el análisis de comportamientos y la detección de ataques fileless, puede detener esta clase de ataques que normalmente sortean la protección de las herramientas antivirus tradicionales.

Atacante:

BITWISE SPIDER

Cuándo
Febrero de 2023

Qué ocurrió
A principios de 2023, CrowdStrike Services respondió a un incidente de **BITWISE SPIDER** LockBit en el que se desplegó la herramienta de filtrado Sender2. El atacante consiguió acceso inicial con credenciales válidas y, a continuación, efectuó el reconocimiento del host y la red mediante herramientas LotL, como `net`, `nltest` y `qwinsta`, que los antivirus tradicionales no identifican como maliciosas.

Cómo ayuda la seguridad de endpoints moderna
En este caso, la seguridad de endpoints moderna habría aplicado análisis para identificar comportamientos poco habituales en herramientas legítimas. Un sistema de seguridad que combina también protección de amenazas para la identidad puede ofrecer una protección adicional, ya que detecta la presencia de ciberdelincuentes que usan cuentas comprometidas o credenciales robadas para conseguir acceso y para moverse lateralmente por los sistemas.

Cambia de solución: las amenazas actuales requieren una seguridad de endpoints moderna

Los ciberdelincuentes han evolucionado y han ideado múltiples formas de evadir la protección de los antivirus tradicionales. Si quieres proteger tu empresa, necesitas seguridad de endpoints moderna.

CrowdStrike es el líder en seguridad de endpoints moderna. **CrowdStrike Falcon® Prevent** es el nuevo estándar en NGAV, y proporciona una protección excelente frente a malware, exploits, intrusiones sin malware y amenazas persistentes avanzadas. La detección y respuesta para endpoints que ofrece **CrowdStrike Falcon® Insight XDR** proporciona una visibilidad global y continua que facilita la detección, la investigación y la respuesta, con el fin de frenar cualquier brecha potencial.

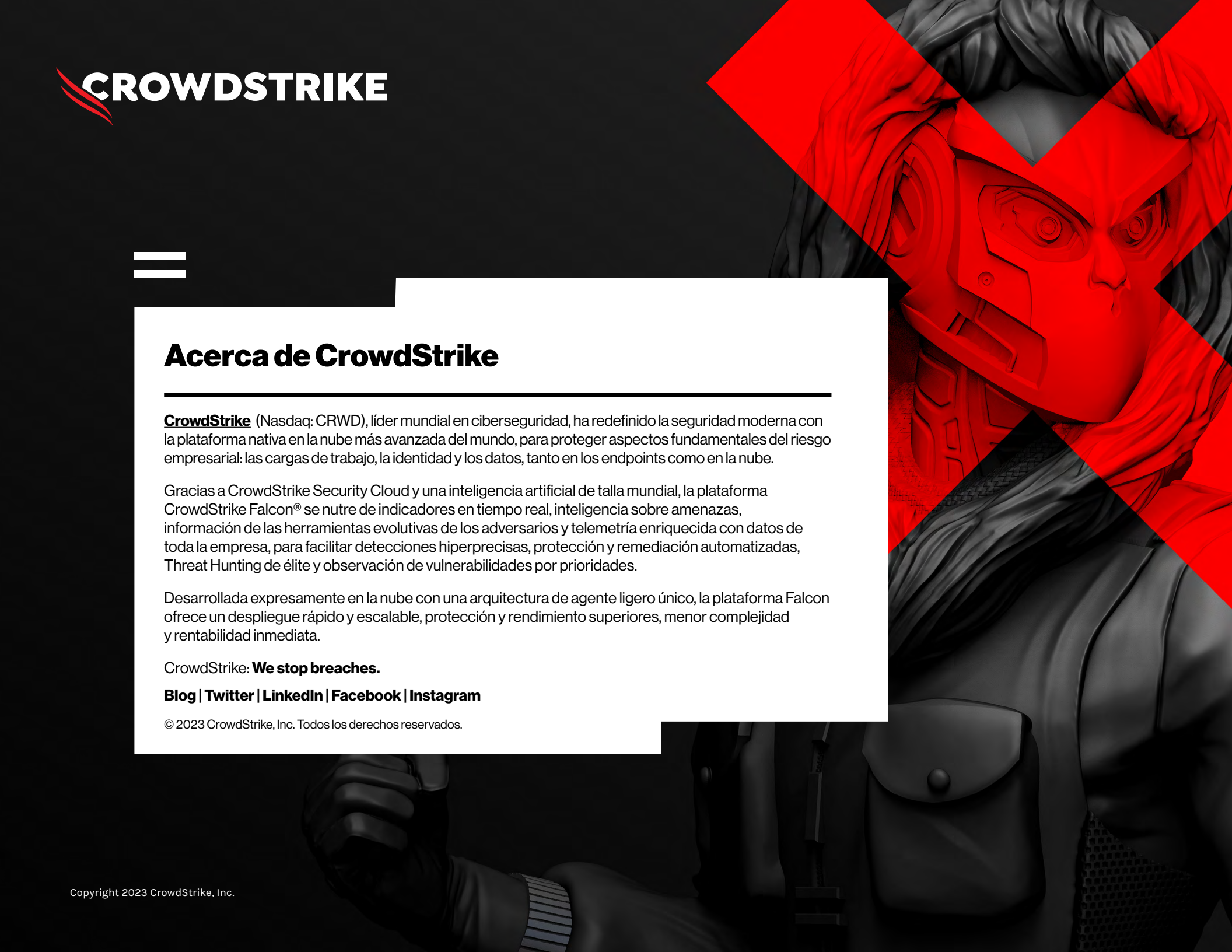
Todas las soluciones de CrowdStrike se despliegan en la plataforma CrowdStrike Falcon® con un solo agente ligero. Este enfoque integrado comprende inteligencia de amenazas, endpoints, identidades y la nube, lo que te permite ampliar fácilmente tu protección a medida que evolucionan las TTP de los ciberdelincuentes.
Una plataforma para protección total.

Pasos siguientes

- **Descubre a los** atacantes interesados en tu sector.
- **Accede** a un kit de herramientas de seguridad de endpoints moderna para obtener otros recursos.
- **Prueba** gratis CrowdStrike Falcon durante 15 días.

"Antes, cuando solo teníamos herramientas antivirus, únicamente contábamos con un cliente grande y agentes que consumían muchísimos recursos. La gestión de estos sistemas requería mucho tiempo y era difícil en las estaciones de trabajo. Sin embargo, CrowdStrike se basa en la nube y solo tiene un agente para todos los módulos de soluciones, a diferencia de otros productos competidores que necesitan varios agentes".

–CISO de Berkshire Bank



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.**

Blog | Twitter | LinkedIn | Facebook | Instagram