Documento técnico de CrowdStrike

CROWDSTRIKE

COMPAS SOLUTIONS

LO QUE CUESTA REALMENTE LA SEGURIDAD DE ENDPOINTS TRADICIONAL

Por qué la seguridad de endpoints moderna mejora la visibilidad y reduce el riesgo

ÍNDICE

LAS SOLUCIONES TRADICIONALES SON INSUFICIENTES PARA LOS EQUIPOS DE SEGURIDAD

Para ser competitivas, las empresas están desarrollando proyectos de transformación digital a través de servicios en la nube. El número de endpoints que se utilizan en estos entornos en dinámica expansión está creciendo vertiginosamente. Según una estimación, la cifra de dispositivos conectados en red en todo el mundo, que en 2018 ascendía a 18 400 millones, alcanzará los 29 300 millones en 2023, un 26 % de ellos dentro del sector empresarial.[1] El perímetro que deben proteger los equipos de seguridad ya supera con creces la red tradicional. Ahora, el contorno de la red está definido por los endpoints, estén donde estén.

¿Permiten las soluciones de seguridad de endpoints tradicionales que los equipos de seguridad protejan los entornos distribuidos dinámicos con éxito frente a las brechas? ¿Son lo suficientemente inteligentes, escalables y flexibles para proteger a las organizaciones de los ataques rápidos, furtivos y complejos que pueden comprometer el acceso a recursos valiosos y a operaciones empresariales cruciales?

Este informe ayuda a los profesionales de la seguridad y de TI a conocer mejor los costos y los riesgos de intentar mejorar la eficacia de las soluciones tradicionales de seguridad de endpoints en el entorno de amenazas actual, así como a entender por qué únicamente una estrategia de protección de endpoints nativa de la nube puede proporcionar la visibilidad, inteligencia, escalabilidad y rapidez que los equipos de seguridad necesitan para conseguirlo.

Según una estimación, la cifra de dispositivos conectados en red en todo el mundo, que en 2018 ascendía a 18 400 millones, alcanzará los 29 300 millones en 2023, un 26 % de ellos dentro del sector empresarial.

Fuente: *"Cisco Annual Internet Report (2018-2023) White Paper"*, Cisco, 9 de marzo de 2020.

SOLUCIONES ANTIVIRUS DISEÑADAS PARA LOS ATAQUES DEL PASADO

Los sistemas de seguridad tradicionales se desarrollaron originariamente para ayudar a los equipos de seguridad a identificar malware basado en archivos. Pero los ciberdelincuentes pronto desarrollaron métodos más sofisticados para llegar a los recursos valiosos con las técnicas siguientes que se utilizan en la actualidad:

- Ataques sin archivos para explotar las vulnerabilidades de plataformas y aplicaciones, en especial los puntos débiles de la seguridad de identidades, lo que supone una amenaza contra las credenciales
- Ataques internos y amenazas persistentes avanzadas gestionadas desde el exterior que dejan puertas traseras y distribuyen ransomware
- Procesos de desarrollo de software comprometidos (por ejemplo, el ataque a la cadena de suministro de SolarWinds descubierto en diciembre de 2020)
  - Un estudio independiente realizado por una firma de investigación del mercado tecnológico concluye que, en opinión del 84 % de los 2200 responsables de toma de decisiones y profesionales de seguridad de TI encuestados, en los tres próximos años, los ataques contra cadenas de suministro podrían convertirse en una de las mayores ciberamenazas para organizaciones como la suya.[2]

Figura 1. Tipos de ataques según su sofisticación

1 *"Cisco Annual Internet Report (2018-2023) White Paper"*, Cisco, 9 de marzo de 2020.
2 *"2021 CrowdStrike Global Security Attitude Survey"*, CrowdStrike, 2021.

En estos ataques, el mejor aliado del ciberdelincuente es la falta de visibilidad que tiene la organización de sus endpoints locales y en la nube. Los endpoints muy distribuidos son difíciles de ver y rastrear, ya que acceden a recursos valiosos y operaciones esenciales que pueden residir localmente, en la nube o en entornos híbridos. La encuesta de Dark Reading sobre el estado de la seguridad de los endpoints reveló que, según el 84 % de los profesionales de seguridad, los ataques siempre empiezan por los endpoints.[3]

La falta de visibilidad prolonga el tiempo necesario para detectar y resolver los ataques, lo que maximiza el daño que los agresores pueden infligir e incrementa el costo de la recuperación. Un estudio realizado en 2021 sobre empresas de las regiones de EE. UU., EMEA y APAC indica que, como promedio, en 2021 las empresas tardaron 146 horas en detectar un incidente de seguridad, frente a 117 horas en 2020 y 120 en 2019.[4]

El reto al que se enfrentan los equipos de seguridad aumenta en la misma medida que el volumen de ataques. Ese mismo estudio mostraba que, en los últimos 12 meses, el 69 % de las organizaciones entrevistadas había sufrido un incidente de ciberseguridad como resultado directo del teletrabajo, el 66 % había recibido al menos un ataque de ransomware y el 45 % había experimentado como mínimo un ataque a la cadena de suministro, cifra que en 2018 fue del 32 %.[5]

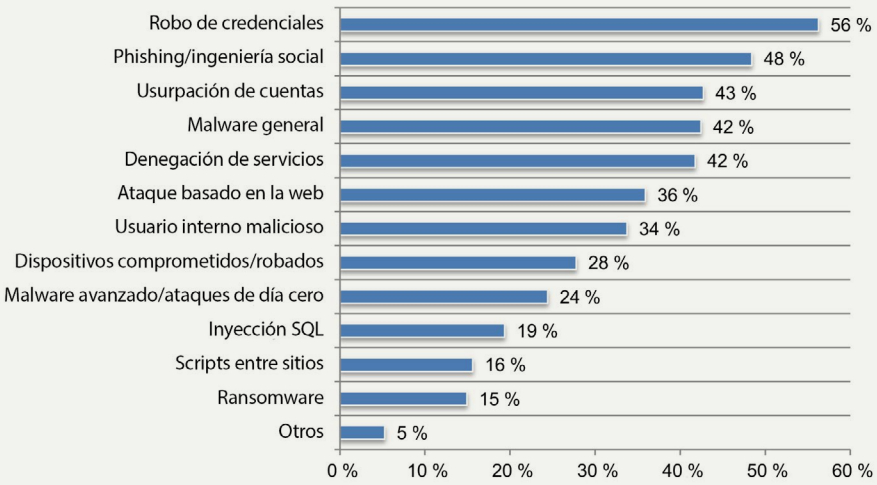
El costo que las empresas soportan por los ataques también es mayor. En 2020, el costo total medio de una fuga de datos ascendió de 3,86 millones de dólares a 4,24 millones, la cifra más alta en los 17 años de historia del informe anual "Cost of a Data Breach Report" del Ponemon Institute.[6] En un informe similar publicado en 2019, el Ponemon Institute descubrió que el costo promedio de un ataque que consigue llegar a los endpoints pasó de 7,1 millones de dólares (en 2018) a 8,94 millones (en 2019).[7]

Para entender la importancia de elegir la mejor manera de proteger a los endpoints en el panorama de amenazas actual, conviene analizar por qué los endpoints son tan vulnerables y qué se precisa para abordar esas vulnerabilidades con el mayor nivel de seguridad posible.

Más allá del malware basado en archivos

El Ponemon Institute encuestó a más de 2200 empleados de TI y seguridad de TI y resumió así los tipos de ataque que habían sufrido:

Figura 10. ¿Qué describe mejor el tipo de ataques experimentados en su organización?
Se permite más de una respuesta



Fuente: *"Cybersecurity in the Remote Work Era: A Global Risk Report"*, Ponemon Institute, octubre de 2020.

Un estudio realizado en 2021 sobre empresas de las regiones de EE. UU., EMEA y APAC indica que, como media, en 2021 las empresas tardaron 146 horas en detectar un incidente de seguridad, frente a 117 horas en 2020 y 120 en 2019.

Fuente: *"2021 CrowdStrike Global Security Attitude Survey"*, CrowdStrike, 2021.

La encuesta de Dark Reading sobre el estado de la seguridad de los endpoints reveló que, según el 84 % de los profesionales de seguridad, los ataques siempre empiezan por los endpoints.

Fuente: *"Endpoint Still a Prime Target for Attack"*, Dark Reading, 24 de septiembre de 2021.

3 *"Endpoint Still a Prime Target for Attack"*, Dark Reading, 24 de septiembre de 2021.
4 *"2021 CrowdStrike Global Security Attitude Survey"*, CrowdStrike, 2021.
5 *"2021 CrowdStrike Global Security Attitude Survey"*, CrowdStrike, 2021.
6 *"Cost of a Data Breach Report 2021"*, Ponemon Institute, 2021.
7 *"The Third Annual Study on the State of Endpoint Security Risk"*, Ponemon Institute, enero de 2020.

UNO DE LOS OBJETIVOS FAVORITOS DE LOS CIBER-DELINCUENTES: LOS ENDPOINTS SIN PROTECCIÓN SÓLIDA

Un endpoint es cualquier dispositivo que puede conectarse a una red para acceder a los recursos y las aplicaciones de una organización. Esta definición no solo incluye estaciones de trabajo y portátiles, sino también servidores y una amplia variedad de dispositivos móviles y conectados a Internet.

Como ha quedado dicho, los endpoints se encuentran allí donde se realiza el trabajo, ya sea en la oficina, en una ubicación remota o en ambas. Y cada uno de ellos es un punto de entrada potencial para un ataque, así como de errores accidentales sin causa malintencionada.

Los endpoints son vulnerables por varias razones importantes.

- Su enorme número, debido a la demanda creciente de teletrabajo y a la continua introducción de nuevos tipos de endpoints, incrementa las posibilidades de éxito de cualquier ataque. Son difíciles de ver y más aún de rastrear.
- Cada endpoint puede ejecutar muchas aplicaciones diferentes con distintas versiones, lo que exige instalar parches y realizar tareas de mantenimiento con regularidad para protegerlos de las vulnerabilidades que los ciberdelincuentes conocen y pueden aprovechar. Cabe decir lo mismo de los sistemas operativos de los endpoints.
- Los empleados llevan a casa endpoints propiedad de la empresa y allí es preciso tener especial cuidado para evitar que otros miembros de la familia los utilicen de forma no segura; además, siguen utilizándose para trabajar dispositivos personales que quizá no son lo suficientemente seguros.

Cuando la seguridad de endpoints es insuficiente, también aumenta el riesgo de daños por errores y uso indebido accidental. Los usuarios finales y los administradores (incluidos los administradores web) se dedican a cumplir las tareas que exige su puesto. Su lista de prioridades no siempre está encabezada por las políticas de seguridad y, si estas son demasiado invasivas, pueden ser hasta contraproducentes, ya que incitan a los usuarios frustrados a buscar el modo de eludirlas.

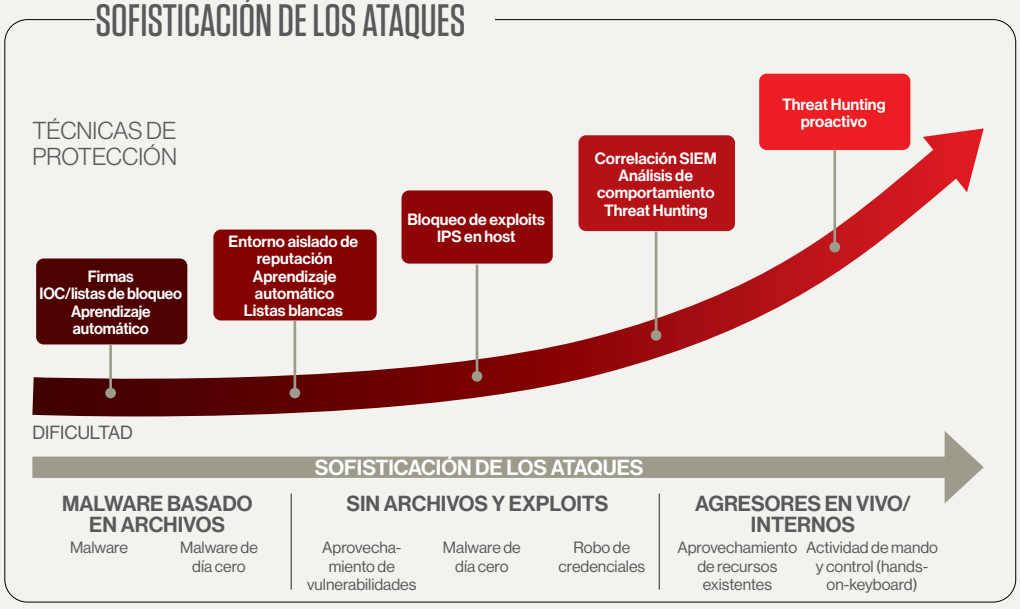


Figura 2. Tipos de técnicas de protección utilizadas para bloquear ataques: la dificultad de protección aumenta con la sofisticación del ataque

Como muestra la Figura 2, la evolución de las amenazas más sofisticadas ha exigido el desarrollo y la introducción de técnicas y tecnologías de protección de endpoints más potentes que pueden ayudar a los equipos de seguridad a:

- Ver con más facilidad lo que ocurre en todos los endpoints, estén donde estén, y hacer posible su ampliación cuando sea necesario
- Conocer y establecer prioridades en el volumen de incidentes y datos de alertas —la mayoría de los cuales son irrelevantes— en relación con lo que sucede en los endpoints
- Investigar y corregir lo que ocurre cuanto antes

Lamentablemente, las soluciones antivirus tradicionales siguen abordando únicamente el tramo inferior de la escala de sofisticación de ataques para el que fueron diseñadas: el malware basado en archivos.

Es importante conocer las funciones de diseño que limitan la utilidad de las soluciones antivirus tradicionales cuando se enfrentan a ataques sofisticados, no solo en el punto de prevención, sino también más allá.

¿EN QUÉ FALLAN LAS SOLUCIONES DE SEGURIDAD DE ENDPOINTS TRADICIONALES?

Las soluciones antivirus tradicionales nunca fueron diseñadas para enfrentarse al entorno ni a los retos actuales de la protección de endpoints. Las soluciones antivirus se centran en la fase de prevención de la seguridad de endpoints, cuyo fin es impedir que las ciberamenazas comprometan el endpoint. Las soluciones antivirus locales centralizadas dependen de un centro de datos que actúa como eje para gestionar los endpoints conectados a través de un agente instalado en cada dispositivo, tanto dentro como fuera del firewall. Al necesitar actualizaciones frecuentes, funcionan en segundo plano y analizan periódicamente el contenido del dispositivo en busca de patrones que coincidan con una base de datos de firmas de virus.

Esta estrategia de protección de endpoints no ofrece la ayuda que necesitan los equipos de seguridad. Las soluciones tradicionales generan:

- **Inflexibilidad operativa.** El sistema tradicional no se actualiza en tiempo real, lo que brinda a los ciberdelincuentes una oportunidad perfecta mientras los equipos de TI instalan parches y despliegan actualizaciones. No ahorran tiempo ni complejidad a unos equipos de seguridad bombardeados por flujos de alertas sin clasificar, ni tampoco se conectan con otras soluciones de seguridad que permitan filtrarlos e investigarlos.
- **Deficiencias de protección.** Con el teletrabajo, la virtualización y la nube, los dispositivos no están siempre conectados a la red corporativa en la que se ejecuta la solución tradicional. Los dispositivos que no están conectados a la red o a Internet pueden ser vulnerables. Cuando se aplican actualizaciones y mejoras, puede haber problemas con el número y el rendimiento de los endpoints.
- **Poca o ninguna ayuda frente a ataques sofisticados.** Las soluciones tradicionales no proporcionan a los equipos de seguridad acceso a información sobre amenazas, algo fundamental para poder reconocerlo todo, desde el malware sin archivos hasta las últimas amenazas persistentes avanzadas. Además, estas soluciones tampoco capacitan a los equipos de seguridad para buscar y aprender proactivamente de amenazas que explotan vulnerabilidades o que roban o utilizan credenciales de forma ilegítima, lo cual puede provocar el acceso indebido a datos y aplicaciones vitales.

ENDPOINTS: MUCHO MÁS QUE ESTACIONES DE TRABAJO Y PORTÁTILES

Los endpoints también incluyen:

- Teléfonos móviles
- Tablets
- Dispositivos conectados a Internet
- Servidores
- Sistemas puntos de venta (PDV)
- Conmutadores
- Impresoras digitales
- Cámaras
- Electrodomésticos
- Relojes inteligentes
- Rastreadores de salud
- Sistemas de navegación

Fuente: **CrowdStrike Cybersecurity 101**

- **Visibilidad limitada.** Las soluciones tradicionales no proporcionan visibilidad real de múltiples dispositivos ni de toda la red, sobre todo cuando los dispositivos de red están desconectados, lo que ofrece a los adversarios la oportunidad de moverse sin ser detectados, en tiempo real. No pueden vigilar suficientemente la actividad de los endpoints ni captar datos importantes para la corrección y el Threat Hunting.
- **Oportunidades para que los ciberdelincuentes traspasen sus barreras.** Con la experiencia, los agresores han llegado a conocer las vulnerabilidades más importantes de las soluciones de seguridad tradicionales y ahora también tienen herramientas para averiguar cómo superar las correcciones que publican los proveedores. Los equipos de seguridad corren un alto riesgo esperando que las soluciones antivirus tradicionales funcionen de formas no contempladas en su diseño. Y el costo que ello conlleva también es elevado.

La renovación de las licencias no representa el verdadero costo de conservar una solución antivirus tradicional en cuanto a personas, procesos y tecnología subyacente.

A nivel corporativo, hay que considerar el costo que acarrea la menor productividad del usuario cuando la sobrecarga de los agentes ralentiza la capacidad de respuesta de miles de endpoints, o las pérdidas que se producen cuando un incidente que el sistema no ha detectado permite una intrusión.

Al conservar un sistema antivirus tradicional, los equipos de seguridad incurren en costos directos, como los de descargar, implementar, configurar y ajustar actualizaciones a menudo frágiles, efectuar los análisis necesarios y realizar tareas de mantenimiento en los servidores locales. Un estudio sobre el impacto económico mostró que un enfoque nativo de la nube y totalmente gestionado de la seguridad de los endpoints puede reducir la carga de la asistencia al eliminar 3,4 empleados a tiempo completo (FTE, por sus siglas en inglés) y generar un ahorro aproximado de 1,5 millones de dólares en tres años.[8]

En lugar de ocuparse de proteger la empresa frente las amenazas más peligrosas, el equipo de seguridad se dedica a bregar con la protección de endpoints de un sistema tradicional que no puede ayudarle a supervisar, clasificar y analizar las alertas de miles de endpoints, lo que le impide responder y corregir con rapidez incidentes que acaban convirtiéndose en brechas.

Así pues, ¿qué proporcionaría los beneficios de una protección de endpoints tradicional y además reduciría las amenazas y los riesgos del entorno actual?

¿QUÉ ES DETECCIÓN Y RESPUESTA PARA ENDPOINTS (EDR)?

Detección y respuesta para endpoints (EDR) es una solución de ciberseguridad que detecta y mitiga las ciberamenazas supervisando continuamente los endpoints y analizando sus datos.

Una verdadera solución EDR ayuda a los equipos de seguridad a:

- Buscar e investigar datos de incidentes
- Clasificar alertas y validar actividades sospechosas
- Detectar actividades sospechosas
- Threat Hunting y analizar datos
- Detener actividades maliciosas

Fuente: **CrowdStrike Cybersecurity 101**

MEJORE LA PROTECCIÓN DE LOS ENDPOINTS CON UNA ESTRATEGIA NATIVA DE LA NUBE

Una plataforma de protección de endpoints nativa de la nube reduce drásticamente los gastos de administración de un sistema tradicional y evita que los equipos de seguridad se enfrenten a las amenazas de ciberseguridad más acuciantes de su empresa. A su vez, los equipos de seguridad ganan:

Resiliencia operativa. Las plataformas nativas de la nube se actualizan en tiempo real y sus algoritmos se ajustan constantemente. La versión utilizada es siempre la última. Los agresores ya no pueden aprovechar el desfase temporal que se produce mientras los equipos de seguridad esperan a que se actualice un sistema tradicional.

8 *"Total Economic Impact™ of CrowdStrike"*, 2021.

Protección siempre disponible y escalable. Las plataformas nativas de la nube funcionan a través de un agente ligero único, por lo que pueden desplegarse inmediatamente en los endpoints y ampliarse rápidamente sin afectar apenas al rendimiento de los endpoints. Cuando los endpoints utilizados para el teletrabajo, la virtualización y la nube pierden conexión con la red corporativa, siguen protegidos.

Un perímetro para ciberdelincuentes sofisticados. Al adoptar un enfoque nativo de la nube para la protección de los endpoints, es posible utilizar nuevas tecnologías de aprendizaje automático e inteligencia artificial que permiten al equipo de seguridad registrar los nuevos ataques, aprender de ellos y aplicar a gran escala la información sobre sus técnicas.

Visibilidad y claridad de todo el espectro en tiempo real. Una plataforma de protección de endpoints nativa de la nube está diseñada para supervisar la actividad de los endpoints y captar continuamente todos sus datos en cualquier lugar. En combinación con la inteligencia sobre amenazas, proporciona contexto para realizar análisis en tiempo real e históricos, así como para implementar Threat Hunting eficaz, ya sea de forma proactiva o gestionada.

Un aliado omnipresente contra los adversarios. Incluso si un ciberdelincuente logra acceder a un sistema, el proveedor de la solución de la plataforma nativa de la nube puede observar sus intentos de desplazarse lateralmente u obtener mayor acceso. En lugar de que los agresores eludan la detección, los defensores pueden observar sus técnicas para mejorar y acelerar la detección.

Una protección de endpoints nativa de la nube puede proporcionar la visibilidad, la inteligencia y la rapidez que los equipos de seguridad necesitan para hacer mejor su trabajo, mientras que las empresas consiguen resiliencia y eficacia operativas al eliminar complejidad en la infraestructura.

DÉ EL PASO SIGUIENTE

¿Preparado para mejorar su protección de endpoints? Hágase con nuestro libro electrónico **"Cinco capacidades esenciales de la seguridad para endpoints moderna: por qué la visibilidad total contribuye a una mejor protección de los endpoints"** para obtener más información sobre lo que debe buscar si quiere mejorar su solución de seguridad de endpoints.

COMPAS SOLUTIONS

ACERCA DE CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), líder mundial en ciberseguridad, ha redefinido la seguridad moderna con una de las plataformas nativas de la nube más avanzadas 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, la plataforma CrowdStrike Falcon® se nutre de indicadores en tiempo real, inteligencia sobre amenazas, herramientas evolutivas de los adversarios y telemetría enriquecida con datos de toda la empresa para facilitar detecciones hiperprecisas, protección y corrección 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 permite que los clientes se beneficien de un despliegue rápido y escalable, protección y rendimiento superiores, menor complejidad y rentabilidad inmediata.

CrowdStrike: **We stop breaches.**

Síganos: **Blog | Twitter | LinkedIn | Facebook | Instagram | https://www.crowdstrike.com/latam/ | latam@crowdstrike.com**