

# Malwarebytes Endpoint Detection & Response



No solo alertamos, sino que arreglamos el problema

La realidad en el panorama de amenazas de hoy en día es que ningún proveedor proporciona una protección del 100 por ciento: [www.malwarebytes.com/remediationmap](http://www.malwarebytes.com/remediationmap).

La violaciones son inevitables. Remediarlas es esencial.

Las organizaciones de hoy en día buscan la manera de abordar los incidentes que sus defensas actuales no manejaron de forma adecuada. Cuando los atacantes eluden las defensas, a menudo transcurren semanas o meses antes de que sean detectados. En 2017, de acuerdo con un estudio global que llevó a cabo el Ponemon Institute, el tiempo promedio para identificar (Mean Time to Identify, MTTI) una violación fue de 191 días.

El propósito de las capacidades de Endpoint Detection and Response (EDR) es acelerar la detección de amenazas y reducir el tiempo de permanencia. Entre más rápido se identifique y contenga una violación de datos, menor será el costo. Las soluciones actuales de EDR identifican la amenaza que eludió la protección tradicional y la respuesta que comúnmente generan es en forma de registros, alertas y correos. Posteriormente, un analista de amenazas usa herramientas para evaluar el código y las máquinas infectadas se restauran.

El enfoque de Malwarebytes Endpoint Detection and Response es diferente. Malwarebytes aprovecha la reparación con Linking Engine y el Ransomware Rollback patentados para ir más allá de las alertas y la restauración, y así corregir el daño. Con Endpoint Detection and Response, usted no tiene que sacrificar la complejidad por el costo.

## CARACTERÍSTICAS TÉCNICAS

### Protección web

Evita el acceso a sitios web maliciosos, redes de anuncios, redes fraudulentas y malos vecindarios.

### Fortalecimiento de aplicaciones

Disminuye la superficie de vulnerabilidades aprovechables y detecta proactivamente los intentos de fingerprinting de ataques avanzados.

### Mitigación de Exploits

Detecta y bloquea proactivamente intentos de aprovechar vulnerabilidades y ejecutar códigos en el punto final de forma remota.

### Protección contra el comportamiento de aplicaciones

Evita que se aprovechen las aplicaciones para infectar el equipo.

### Aprendizaje automático de detección de anomalías

Identifica proactivamente virus y malware mediante técnicas de aprendizaje automático.

### Análisis de cargas útiles

Identifica familias completas de malware conocido y relevante con reglas heurísticas y de comportamiento.

### Mitigación del ransomware

Detecta y bloquea ransomware mediante tecnología de supervisión de comportamiento.

### Reparación con Linking Engine

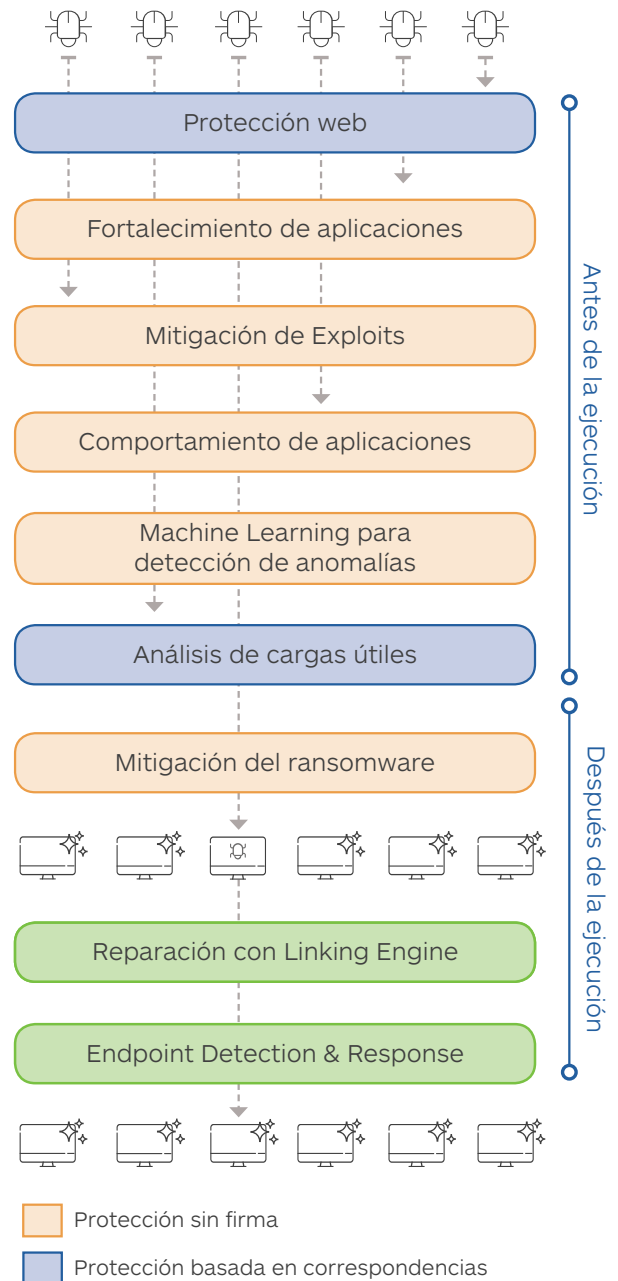
Proporciona una reparación completa y exhaustiva para que el equipo regrese a un estado verdaderamente sano mientras minimiza el impacto en el usuario final.

### Endpoint Detection and Response (EDR)

Visibilidad en los equipos para análisis forense y de comportamiento continuos. Reduce el tiempo de permanencia a cero amenazas al día. Proporciona opciones de respuesta más allá de las alertas.



## ENDPOINT DETECTION & RESPONSE



## Beneficios claves

### Protección en varias capas

La protección multivectorial de Malwarebytes (Multi-Vector Protection, MVP) usa un enfoque de siete capas, que incluye técnicas de detección dinámicas y estáticas, para proteger durante todas las etapas de un ataque. Este enfoque proporciona protección contra todo tipo de amenazas, desde los virus tradicionales hasta las amenazas avanzadas del futuro.

### Visibilidad en los equipos para un monitoreo continuo

Flight Recorder proporciona un monitoreo y una visibilidad continuos en los escritorios de Windows para obtener información poderosa. Puede dar seguimiento fácilmente a la actividad del sistema de archivos, la actividad de red, la actividad de proceso y la actividad de registro. Los eventos de Flight Recorder se almacenan localmente y en la nube.

### Tres modos de aislamiento de equipos

Cuando un equipo comprometido, Malwarebytes detiene la infiltración aislando el equipo. La corrección rápida previene el movimiento lateral. Detiene el avance del malware y bloquea a los atacantes remotos. Endpoint Protection and Response es el primer producto que ofrece tres formas de aislar un equipo. Aislamiento de red para restringir los procesos que se pueden comunicar. Aislamiento de procesos para restringir los procesos que se pueden ejecutar. Aislamiento de escritorio para alertar al usuario final y poner alto a la interacción. Mantiene al sistema en línea de manera segura para hacer un análisis detallado.

### Reparación completa y exhaustiva

Malwarebytes proporciona la reparación más confiable de la industria, como lo demuestran las 500,000 descargas y la reparación de 3 millones de infecciones al día en todo el mundo. Malwarebytes Endpoint Protection and Response aprovecha la tecnología de Malwarebytes Linking Engine para eliminar todos los rastros de infecciones y artefactos relacionados, y no solamente la carga de la amenaza principal. Este enfoque ahorra el tiempo que por lo general se invierte en borrar y restaurar equipos.

### Ransomware Rollback

La tecnología de Ransomware Rollback le permite retroceder el reloj para anular el impacto del ransomware aprovechando los respaldos que se hicieron justo a tiempo. Malwarebytes registra y asocia cambios con procesos específicos. Cada cambio hecho por un proceso se registra. Si un proceso hace cosas "malas", puede retroceder fácilmente esos cambios para restaurar los archivos que se encriptaron, borraron o modificaron. El almacenamiento de datos se minimiza al usar tecnología patentada de exclusión dinámica que aprende lo que hacen las aplicaciones "buenas".

### Administración centralizada en la nube

Reduce la complejidad a la vez que facilita la implementación y la administración, sin importar el número de equipos. Además, elimina la necesidad de adquirir y mantener hardware en el lugar.



**DISTRIBUIDOR EN MEXICO**

**JEVC Multimedia & e-Business**

malwarebytes@softwaredeseguridad.mx

www.softwaredeseguridad.mx

Teléfono: 642 422 4238



malwarebytes.com/business

Malwarebytes es una empresa de ciberseguridad que tiene la confianza de millones de personas de todo el mundo. Malwarebytes protege proactivamente a personas y empresas contra las amenazas maliciosas, incluido el ransomware, que los antivirus tradicionales no detectan. El producto insignia de la empresa usa tecnologías sin firma para detectar y detener un ciberataque antes de que ocasione daños. Conozca más en [www.malwarebytes.com](http://www.malwarebytes.com).

Copyright © 2018, Malwarebytes. Todos los derechos reservados. Malwarebytes y el logotipo de Malwarebytes son marcas registradas de Malwarebytes. Las demás marcas pueden ser propiedad de otros. Todas las descripciones y especificaciones del presente están sujetas a cambio sin previo aviso y se proporcionan sin garantía de ningún tipo.