

# Malwarebytes Endpoint Security

Prevención avanzada de amenazas



Malwarebytes Endpoint Security es una plataforma de protección de equipos que utiliza múltiples tecnologías para proteger proactivamente sus computadoras frente a amenazas conocidas y desconocidas. La protección contra ataques en múltiples etapas proporciona a empresas de cualquier tamaño y sector, en todo el mundo, la capacidad de detener a los cibercriminales en todas las etapas de la cadena de ataque.

## Beneficios clave

### Detiene los ataques avanzados de malware y ransomware

Reduce las posibilidades de que se filtren datos y ahorra recursos de IT al proteger contra ciberamenazas que la seguridad tradicional puede pasar por alto.

### Protege contra exploits y ransomware

Protege los programas que no reciben soporte al blindar sus vulnerabilidades contra exploits. La tecnología de supervisión de comportamiento no basada en firmas detecta y bloquea automáticamente el ransomware desconocido (de tipo hora cero).

### Aumenta la productividad

Protege la productividad del usuario final al preservar el rendimiento del sistema y mantener al personal en los proyectos que producen ingresos.

### Administración sencilla

Simplifica la administración de la seguridad de los equipos e identifica los que son vulnerables. Agiliza la implementación de la seguridad de los equipos y optimiza el uso de los recursos de administración de IT.

### Prevención de amenazas escalable

Brinda protección en todos los equipos, extendiéndose fácilmente a medida que su empresa crece.

### Detecta sistemas desprotegidos

Descubre todos los equipos y el software instalado en su red. Los sistemas sin Malwarebytes que son vulnerables a los ciberataques se pueden asegurar fácilmente.

### Asegura los equipos Mac

Proporciona protección en tiempo real para equipos de macOS y detecta y repara malware, incluido el adware.\*

### Protege los dispositivos Android

Ofrece múltiples capas de protección en tiempo real para dispositivos con el sistema operativo Android. Bloquea llamadas maliciosas y analiza mensajes de texto SMS en busca de amenazas de phishing.\*

*\*La protección en tiempo real de macOS, la protección de dispositivos móviles con Android y los clientes de reparación independientes no se administran desde la consola central de administración.*

## PRINCIPALES TECNOLOGÍAS

### Anti-malware

Prevención avanzada de malware

### Anti-exploit

Cuatro capas de protección de exploits

### Anti-ransomware

Detecta y bloquea automáticamente el ransomware

### Management Console

Implementación y administración centralizada, políticas de seguridad e informes a través de la consola de administración en las propias instalaciones

## PREMIOS

### Gartner

Malwarebytes es reconocido como un visionario en el Gartner Magic Quadrant for Endpoint Protection Platforms de 2018

### FORRESTER®

Malwarebytes es nombrado "Strong Performer" en el informe The Forrester Wave: Endpoint Security Suites, Q2 2018

## Características

- ▶ Análisis proactivo anti-malware y anti-spyware
- ▶ Tres modos de análisis del sistema (rápido, flash y completo)
- ▶ Bloqueo de sitios web maliciosos
- ▶ Bloqueo de ejecución de archivos
- ▶ Tecnología Malwarebytes Chameleon
- ▶ Opción de eliminar al reiniciar

## Anti-exploit

### Características

- ▶ Protección contra grietas en la seguridad del sistema operativo
- ▶ Protección para ejecución desde memoria
- ▶ Protección de comportamiento de aplicaciones
- ▶ Fortalecimiento de aplicaciones

## Anti-ransomware

### Características

- ▶ Motor especializado para detección y bloqueo en tiempo real
- ▶ Tecnología exclusiva de comportamiento de ransomware
- ▶ Identificación de ransomware no identificado (de tipo hora cero) no basada en firmas
- ▶ Requiere de pocos recursos del sistema
- ▶ Compatible con soluciones de seguridad de terceros

## Management Console

### Características

- ▶ Administración escalable en sus instalaciones con funcionalidad de instalación de forma remota
- ▶ Programación flexible de análisis
- ▶ Vista de amenazas con informes centralizados
- ▶ Simulador virtual de implementación
- ▶ Integración de Active Directory

## REQUISITOS DEL SISTEMA

### Equipos

Sistemas operativos compatibles:

Windows 10, 8.1, 8, 7\*, Vista, XP  
Windows Server 2016, 2012, 2008, 2003  
Windows Small Business Server 2011  
MacOS (10.10) y posterior (no administrado)  
Android 4.4 (KitKat) y posterior  
(no administrado)

### Hardware:

CPU de 800 MHz o superior  
1 GB de RAM o superior (2 GB o superior para Windows Server)  
35 MB de espacio libre en disco

### Management Console

Sistemas operativos compatibles:  
Windows Server\* 2016, 2012, 2008

Versiones de Microsoft SQL

Server compatibles:

SQL Server 2016, 2014, 2012, 2008  
SQL Server 2008 Express (incluido con el producto)

### Hardware:

CPU de 2 GHz (se recomienda procesador con doble núcleo a 2.6 GHz o superior)  
2 GB de RAM o superior (se recomiendan 4 GB)  
10 GB de espacio libre en disco  
(se recomiendan 20 GB)

\*Las funciones anti-ransomware son compatibles con Windows 7 y superior. No son compatibles con Windows Server.

## DISTRIBUIDOR EN MEXICO

**JEVC** Multimedia  
& e-Business

malwarebytes@softwaredeseguridad.mx

www.softwaredeseguridad.mx

Teléfono: 642 422 4238



malwarebytes.com/business

Malwarebytes protege proactivamente a personas y empresas contra amenazas peligrosas como malware, ransomware y exploits que los antivirus tradicionales no detectan. Malwarebytes sustituye completamente a los antivirus con tecnología de inteligencia artificial que detiene los ciberataques antes de que puedan comprometer los equipos domésticos y corporativos. Más información en <http://www.malwarebytes.com>.