Malwarebytes™ for Business

GUÍA COMPARATIVA

MALWAREBYTES
CARTERA EMPRESARIAL

Soluciones de Endpoint Security	Malwarebytes Incident Response	Malwarebytes Endpoint Protection	Malwarebytes Endpoint Detection and Response
DESINFECCIÓN DE AMENAZAS			
Análisis de amenazas bajo demanda y programadas, desinfección soluble Malwarebytes Breach Remediation (MBBR)	✔	✔	✔
PREVENCIÓN DE AMENAZAS			
Protección contra manipulaciones Requiere que los usuarios proporcionen una contraseña al intentar desinstalar Malwarebytes Endpoint Agent Software	✔	✔	✔
Monitoreo de la salud Permite que Malwarebytes Endpoint Agent Monitor Service lleve a cabo un monitoreo y reinicie el Endpoint Agent Service si pierde la conexión o se detiene.	✔	✔	✔
Control de dispositivos USB Establezca los permisos de acceso para los dispositivos de almacenamiento masivo USB en Bloquear, Permitir o Solo lectura		✔	✔
PROTECCIÓN MULTIVECTORIAL: capas de tecnologías Malwarebytes para detener un ataque en cualquier punto de la cadena de ataque			
Protección web Ayuda a evitar el acceso a sitios web maliciosos, redes de anuncios, redes fraudulentas		✔	✔
Fortalecimiento de aplicaciones Disminuye la superficie de vulnerabilidad de los exploits y detecta proactivamente los intentos de fingerprinting de ataques avanzados		✔	✔
Mitigación de exploits Detecta y bloquea proactivamente intentos de aprovechar vulnerabilidades y ejecutar código en el terminal de forma remota		✔	✔
Protección de comportamiento de aplicaciones Ayuda a evitar que se aprovechen las aplicaciones para infectar el terminal		✔	✔
Machine Learning de detección de anomalías Identifica proactivamente virus y malware desconocidos mediante técnicas de Machine Learning		✔	✔
Análisis de carga maliciosa Tecnología antimalware diseñada para identificar familias completas de malware conocido y relevante con reglas heurísticas y de comportamiento		✔	✔
Mitigación del ransomware Detecta y bloquea ransomware mediante tecnología de monitoreo del comportamiento		✔	✔
Protección de ataques por fuerza bruta Protección para terminales Windows frente a conexiones sospechosas a través de dispositivos remotos		Escritorio y servidor Windows	Escritorio y servidor Windows

Soluciones de Endpoint Security

	Malwarebytes Incident Response	Malwarebytes Endpoint Protection	Malwarebytes Endpoint Detection and Response
CAZA DE AMENAZAS, AISLAMIENTO Y RECUPERACIÓN			
Monitoreo de actividades sospechosas Monitoreo continuo y visibilidad de eventos del sistema de archivos del terminal, conexiones de red, eventos de procesos y actividad del Registro			✔
Búsqueda de Flight Recorder Caza de amenazas de forma libre en todos los dispositivos gestionados por EDR			✔
Sandbox en la nube integrado Los archivos binarios nunca antes vistos (únicos y nuevos) se detonan automáticamente en un entorno virtual seguro y aislado. Los resultados enriquecen los datos presentados en Actividades sospechosas.			✔
Endpoint Isolation Aislamiento de redes, procesos y escritorios diseñado para impedir que el malware se comunique y bloquear el acceso a atacantes remotos			✔
Ransomware Rollback Hasta 72 horas de protección para los archivos cifrados, eliminados o modificados por un ataque de ransomware			✔
Mapeo de MITRE ATT&CK Destaca cómo las reglas de detección de Malwarebytes encajan en el marco de MITRE ATT&CK			✔
Active Response Shell Recuperación remota del código sospechoso y utilización de Forensic Timeliner para investigación y registro			✔
ADMINISTRACIÓN			
Consola de gestión centralizada	✔	✔	✔
SEGURIDAD MÓVIL			
Extiende nuestra potente protección de endpoints a sus dispositivos móviles, protegiéndolos de las más recientes amenazas móviles como ransomware, aplicaciones nocivas y programas potencialmente no deseados (PUP). Con protección en tiempo real para sus dispositivos móviles, puede evitar un acceso accidental a sitios web nocivos, protegerse de aplicaciones nocivas y bloquear anuncios no deseados.	**Sistemas operativos compatibles**: Android, Chromebooks e iOS 		

Managed Detection and Response

	Malwarebytes Managed Threat Hunting (MTH)	Malwarebytes Managed Detection & Response (MDR)
Monitoreo, análisis, orientación e investigación las 24 horas del día durante todo el año		✔
Detección personalizada de amenazas las 24 horas del día durante todo el año		✔
Campaña activa de detección de amenazas las 24 horas del día durante todo el año	✔	✔
Reparación experta de endpoints las 24 horas del día durante todo el año		✔
Orientación para realizar la reparación las 24 horas del día durante todo el año	✔	✔
Uso de inteligencia acerca de amenazas de múltiples fuentes	✔	✔
Revisión retrospectiva de 31 días de indicadores de riesgo (IOC) críticos		✔
Notificaciones a través de los portales Nebula / OneView y notificaciones por niveles basadas en la gravedad del incidente	✔	✔
Informes mensuales sobre la prestación de servicios		✔
Integración con los Administradores de cuentas (AM) para las Revisiones trimestrales de negocios (QBR)		✔
Incorporación de clientes con atención personalizada y de alta calidad		✔
Modelo de licencia	Suscripción	Suscripción

Servicios

SERVICIO DE ELIMINACIÓN DE MALWARE	
Nuestros expertos del sector ayudan a acelerar la recuperación de su organización de un incidente. Trabajando de forma remota, brindamos un servicio integral desde la respuesta crítica inicial hasta la reparación completa que se encarga de sus necesidades inmediatas de eliminación de malware.	**Fases de contratación de servicios** • Alcance del proyecto • Revisión del entorno • Asistencia para la implementación • Confirmación de reparación y transferencia de conocimientos

Soporte

	Soporte Estándar	Soporte Estándar Plus
Teléfono, correo electrónico y chat	✔	✔
Soporte las 24 horas del día para el nivel de gravedad 1		✔
Direccionamiento de casos prioritario		✔
Acceso a la base de conocimientos, la comunidad, las guías de productos y la capacitación en línea de Malwarebytes Academy	✔	✔
ADMINISTRACIÓN TÉCNICA DE CUENTAS		
Obtenga una relación proactiva y de asesoramiento con su administrador técnico de cuentas (TAM) asignado para que le ayude a aprovechar al máximo el valor de sus soluciones de Malwarebytes y optimizar sus niveles de servicio de TI. Los servicios TAM de Malwarebytes proporcionan recursos de seguridad proactivos para la defensa del cliente y un técnico colaborador para ayudarle a optimizar su perfil de seguridad.	Servicio complementario que incluye soporte Estándar Plus	

Módulos de ciberseguridad

VULNERABILITY ASSESSMENT	
Le ayuda a identificar, clasificar y priorizar vulnerabilidades en controladores, aplicaciones, sistemas operativos (SO) de servidores y escritorios macOS y Windows al comparar los resultados de sus escaneos automáticos con un inventario actualizado del software en su entorno de TI. Con Vulnerability Assessment, puede programar análisis que descubran actualizaciones pendientes o versiones obsoletas de su software.	**Sistemas operativos compatibles**: Windows y MacOS
PATCH MANAGEMENT	
Automatiza y acelera la implementación y verificación de revisiones de código de software en sistemas operativos y una amplia gama de aplicaciones modernas y heredadas de terceros, incluidas Adobe, Chrome y aplicaciones de almacenamiento en la nube (como Box). Con Patch Management, puede programar la implementación de parches y crear informes resumidos para ayudarle a cumplir con sus requisitos de gobernanza, regulación de datos y seguros cibernéticos.	**Sistemas operativos compatibles**: Windows
DNS FILTERING	
Le permite bloquear sitios que presentan riesgos y obstaculizan la productividad para que pueda proteger mejor a los usuarios finales y sus aplicaciones basadas en web. DNS Filtering le ayuda a garantizar que sus usuarios finales estén más seguros y sean más productivos en la web al filtrar categorías enteras de sitios inapropiados, dominios sospechosos conocidos y otros contenidos peligrosos para que no causen estragos en su negocio.	**Sistemas operativos compatibles**: Windows
SERVICIO DE CLOUD STORAGE SCANNING	
Ayuda a simplificar la tarea de monitoreo, protección y elaboración de informes sobre la seguridad de los datos almacenados en varios repositorios en la nube, incluidos Box y OneDrive. Cloud Storage Scanning utiliza un enfoque exclusivo con múltiples motores e independiente del proveedor, que está diseñado específicamente para detectar amenazas conocidas y desconocidas en archivos almacenados en la nube.	**Proveedores de almacenamiento de información compatibles:** Box, OneDrive y Google Drive *Disponible próximamente*: Dropbox y AWS S3
APPLICATION BLOCK	
Le permite identificar y bloquear fácilmente aplicaciones que son amenazas conocidas o simplemente innecesarias en el lugar de trabajo, sin aumentar la complejidad de la administración de la seguridad. Nuestro módulo Application Block amplía nuestra plataforma de seguridad basada en la nube, bloqueando aplicaciones que pueden representar un riesgo o disminuir la productividad con el fin de proteger mejor a los usuarios finales.	**Sistemas operativos compatibles**: Windows

Malwarebytes cree que, cuando las personas y organizaciones no tienen que preocuparse por las amenazas, pueden prosperar. Además de la desinfección de malware, la empresa ofrece ciberprotección, privacidad y prevención a decenas de miles de usuarios y organizaciones cada día. Para obtener más información, visite https://es.malwarebytes.com/.