Malwarebytes

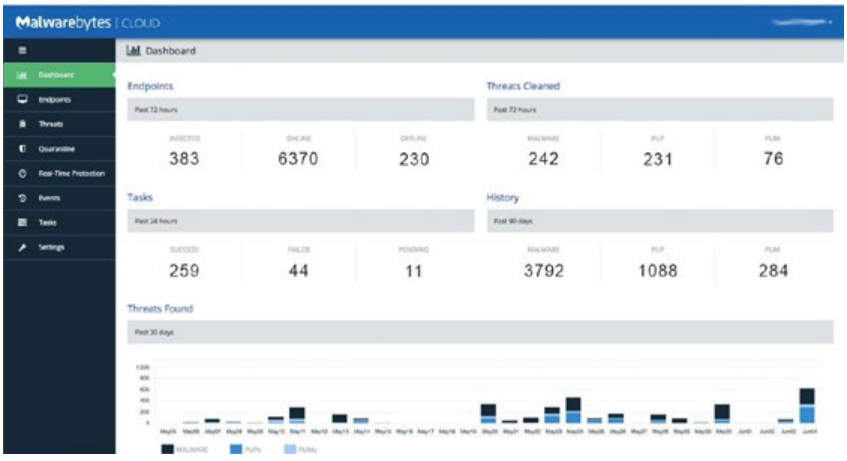
HOJA DE DATOS

Malwarebytes **Incident Response**

Detección y desinfección centralizadas de amenazas

Los atacantes modernos están sofisticando la forma de obtener información de sus víctimas y de llevar a cabo sus ciberataques. Los ataques maliciosos continúan penetrando en la red aunque las empresas, colegios y organismos gubernamentales hayan invertido miles de millones en reforzar sus sistemas de seguridad. Se requiere mucho tiempo y grandes esfuerzos para responder a estos incidentes[1]; a menudo se tarda entre 6 y 8 horas en desinfectar o restaurar un solo terminal. Según investigaciones del Ponemon Institute, se tarda una media de 229 días en identificar los ataques maliciosos o delictivos y 82 días en frenarlos[2]. Las empresas deben armar a sus equipos de seguridad con la telemetría mejor informada y las mejores soluciones de desinfección.

Malwarebytes Incident Response es una herramienta de detección y desinfección basada en una plataforma de gestión en la nube altamente adaptable. Analiza los terminales de la red para detectar amenazas avanzadas como malware, PUP y adware, y las elimina por completo. Malwarebytes Incident Response mejora la detección de amenazas y el tiempo que se tarda en responder a un ataque con las ventajas añadidas de la adaptabilidad, la flexibilidad y la automatización.



Menú principal de la consola en la nube de Malwarebytes

CARACTERÍSTICAS TÉCNICAS

INCIDENT RESPONSE

Motor Incident Response
Análisis de amenazas rápido y sumamente efectivo con opciones a demanda, programadas y automatizadas

Varios modos de análisis
Los modos de análisis Hyper, Amenazas y Personalizado no interrumpen a los usuarios finales

Linking Engine
La tecnología sin firmas identifica y elimina por completo todos los artefactos amenazantes asociados a la carga maliciosa principal

Plataforma en la nube Malwarebytes
La consola de gestión en la nube permite gestionar la política de seguridad y llevar a cabo las instalaciones y la notificación de amenazas de forma sencilla y centralizada

Gestión de recursos
Proporciona detalles útiles sobre el sistema terminal, como objetos de memoria, software instalado, programas de arranque y mucho más

Forensic Timeliner
Recopila y organiza eventos de registro de Windows en una única vista cronológica

Referencias

[1]Incident response se refiere por lo general al conjunto de herramientas, procesos y talentos que usan las organizaciones para combatir y mitigar un ciberataque tras su identificación.

[2]Fuente: Ponemon Institute, 2016 Cost of Data Breach Study, junio de 2016.

Principales ventajas

Automatización

Puede preinstalar Malwarebytes Incident Response en sus terminales para tener una detección y desinfección de amenazas avanzada con un simple clic. También se integra en sus sistemas existentes de gestión de terminales y de gestión de la información y los eventos de seguridad (SIEM) y en sus herramientas de detección de amenazas para responder de forma automática ante las alertas de incidentes. Con la automatización de respuestas ante amenazas, las empresas pueden acelerar sus flujos de trabajo de respuesta ante incidentes y reducir el tiempo de permanencia de los ataques.

Flexibilidad

Malwarebytes Incident Response usa un agente persistente y también incluye opciones de agentes no persistentes (Breach Remediation). Esto aporta unas opciones de instalación flexibles para diversos entornos informáticos empresariales. Malwarebytes se integra fácilmente en su sistema de seguridad y cumple los requisitos de su sistema operativo (Windows y Mac OS X) y de su infraestructura.

Adaptabilidad

Malwarebytes Incident Response está disponible en nuestra nueva plataforma de gestión de terminales en la nube de Malwarebytes. La plataforma en la nube de Malwarebytes reduce la complejidad y facilita la instalación y la gestión de Malwarebytes Incident Response y de otras soluciones Malwarebytes, tanto si tiene un millón de terminales como si tiene un solo terminal. Esta consola centralizada en la nube acaba con la necesidad de adquirir y mantener el hardware en su empresa.

REQUISITOS DEL SISTEMA

Componentes incluidos:
Plataforma en la nube Malwarebytes
Malwarebytes Incident Response (agentes persistentes de Windows y Mac OS X)
Breach Remediation (agentes no persistentes de Windows con CLI y de Mac con GUI y CLI)
Forensic Timeliner (Windows)
Asistencia por correo electrónico y telefónica

Requisitos de hardware
Windows
CPU: 1 GB (clientes); 2 GB (servidores)
Espacio disponible en disco: 100 MB (programa + registros)
Conexión a Internet activa
Mac
Cualquier dispositivo Apple Mac que sea compatible con la versión
10.10 o superior de Mac OS X
Conexión a Internet activa

Sistemas operativos compatibles
Windows 10® (32 bits, 64 bits)
Windows 8.1® (32 bits, 64 bits)
Windows 8® (32 bits, 64 bits)
Windows 7® (32 bits, 64 bits)
Windows Vista® (32 bits, 64 bits)
Windows XP® con SP3 (solo 32 bits)
Windows Server 2016® (32 bits, 64 bits)
Windows Server 2012/2012R2® (32 bits, 64 bits)
Windows Small Business Server 2011
Windows Server 2008/2008R2® (32 bits, 64 bits)
Windows Server 2003® (solo 32 bits)

Tenga en cuenta que los servidores de Windows que utilizan el proceso de instalación Server Core están expresamente excluidos.

La integración con Windows Action Center no es compatible con sistemas operativos Windows Server.

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes es la compañía de seguridad informática de última generación en la que confían millones de personas de todo el mundo. Malwarebytes protege de forma proactiva a particulares y empresas frente a amenazas peligrosas como malware, ransomware y exploits que las soluciones antivirus tradicionales no logran detectar. El producto estrella de la empresa combina la detección heurística de amenazas avanzadas con la tecnología sin firmas para detectar y detener ciberataques antes de que se produzcan daños. Más de 10 000 empresas de todo el mundo usan y recomiendan Malwarebytes como software de confianza. Fundada en 2008, la empresa tiene su sede principal en California y oficinas en Europa y Asia, y cuenta con un equipo global de investigadores y expertos en seguridad.