

# Vermeer implementa sistemas de detección frente al malware a nivel industrial

El equipo de seguridad usa Malwarebytes Endpoint Security para desinfectar y prevenir nuevas infecciones, además de simplificar la vigilancia y el análisis remotos

## SECTOR

Fabricantes

## DESAFÍO COMERCIAL

Formalizar el plan de seguridad de la empresa y añadir una nueva capa de protección en los terminales

## ENTORNO DE TI

Centro de datos con soluciones de seguridad empresariales, incluidos firewalls, seguridad perimetral, filtrado web, filtrado de correos electrónicos y spam y software antivirus

## SOLUCIÓN

Malwarebytes Endpoint Security, que incluye Anti-Exploit, Anti-Malware y la consola de administración

## RESULTADOS

- Los resultados de los análisis se reciben un 50 por ciento más rápido que anteriormente
- Consecución de una detección, bloqueo y eliminación proactivos del malware
- Eliminación del malware y mejora del rendimiento de los terminales
- Mejora significativa de la eficacia de la administración

## Perfil de la empresa

Vermeer ofrece equipos industriales y agrícolas diseñados para el trabajo duro, para tener un gran rendimiento y para aportar valor, y están respaldados por un atento servicio al cliente proporcionado a través de una red global de distribuidores. Cuando llegó la hora de que la empresa formalizara sus directivas de seguridad y añadiera protección frente al malware y los exploits, buscaron un producto que se equiparara en potencia a los productos que fabrican.

*Sé que Malwarebytes permite ahorrar tiempo y que los equipos de nuestros empleados funcionan mejor. Vermeer ha dado los pasos correctos e implementado los procedimientos recomendados para proteger a los usuarios de los terminales.*

—Michael Kraft, ingeniero de Seguridad de TI, Vermeer

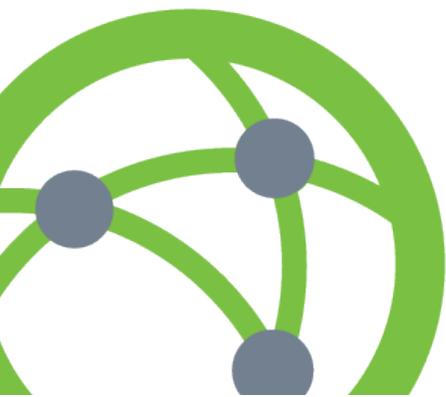
## Desafío comercial

Implementar sistemas de seguridad de clase industrial con fácil administración por parte de un único propietario

Vermeer es una compañía global con sede central en Pella, Iowa, y filiales en Dakota del sur, China, Singapur, Países Bajos y Brasil. El equipo de TI da soporte a los empleados de Vermeer de todo el mundo y Michael Kraft, Ingeniero de seguridad de TI en Vermeer, es el encargado de proteger a la organización frente a las amenazas informáticas como, por ejemplo, el malware.

Como parte fundamental de una iniciativa para actualizar y formalizar el plan de seguridad de la empresa, Kraft era consciente de que una capa adicional de seguridad en los terminales era recomendable. El anterior software antivirus elegido por Vermeer controlaba los virus de forma eficaz pero el malware acabó entrando a pesar de todo. El producto de seguridad de redes perimetrales de la empresa alertaba al equipo cada vez que eso sucedía.

«Recibíamos lo que yo llamo malware "molesto" cada semana», afirma Kraft. «Recibíamos barras de herramientas, adware, programas potencialmente no deseados e incluso, algunas veces, algún empleado descargaba archivos maliciosos sin darse cuenta. Yo era capaz de solucionar los problemas, pero necesitábamos una solución que pudiera detectar y evitar las infecciones desde el primer momento».



Kraft probó otra solución para terminales especializada en malware, pero era desesperadamente lenta y carecía de potentes características de administración remota. Cuando Kraft recibía una alerta, quería diagnosticar y solucionar el problema con rapidez desde donde se encontrara en ese momento. Conocía Malwarebytes de experiencias anteriores, pero quería evaluar otras posibles soluciones a nivel industrial para elegir la más adecuada.

Como antiguo realizador de pruebas de intrusión, Kraft realizó una prueba de concepto para someter a Malwarebytes Endpoint Security a todas las comprobaciones. Después de probar los sistemas, seleccionó Malwarebytes Endpoint Security para Vermeer.

«Al principio pensamos en utilizar Malwarebytes únicamente para la desinfección», asegura, «pero cuando vimos la consola de administración, nos dimos cuenta de que aceleraba y simplificaba la administración. Además, si necesitaba ver un equipo, analizar o reparar un sistema cuando me encontraba de viaje, podía hacerlo de forma rápida y sencilla».

## La solución

### Malwarebytes Endpoint Security

Malwarebytes Endpoint Security, que incluye Anti-Malware for Business, Anti-Exploit for Business y la consola de administración. Malwarebytes Anti-Malware for Business reduce las vulnerabilidades por malware de hora cero mediante unas potentes características de detección y reparación. Malwarebytes Anti-Exploit for Business permite proteger los terminales con una defensa en capas diseñada para derrotar al malware más reciente y peligroso, incluido el ransomware.

### Mayor visibilidad

«Malwarebytes confirmó mis sospechas sobre la cantidad de malware que se encontraba oculto bajo la superficie», asegura Kraft. «La primera vez que implementamos Malwarebytes, encontramos un montón de procesos en nuestros terminales que estaban afectando al rendimiento. Y ninguno de ellos hizo saltar las alarmas».

Después de implementar análisis diarios y semanales, la lista de amenazas de Kraft se ha ido reduciendo drásticamente. Malwarebytes impide que entre prácticamente todo el malware y facilita la limpieza en el caso de que un usuario haya descargado un archivo malicioso sin saberlo.

### Detección y bloqueo proactivos

Al tratarse de un motor de análisis proactivo frente al malware, Malwarebytes permite bloquear los sitios web maliciosos y detectar y reparar las amenazas de malware antes de que se produzcan infecciones más graves. La detección y el bloqueo proactivos le permiten ahorrar tiempo a Kraft y le indican rápidamente los posibles problemas que necesitan una intervención. Malwarebytes permite también poner en cuarentena o eliminar el malware detectado, dependiendo de las directivas que se hayan implementado.

«Generábamos varios informes para nuestras reuniones trimestrales y los informes de Malwarebytes proporcionaban unos datos precisos», asegura. «Eran increíbles porque mostraban a simple vista nuestra eficacia a la hora de atacar y vitar el malware con la ayuda de Malwarebytes».

### Administración remota rápida y sencilla

«Tengo la consola de administración de Malwarebytes en mi pantalla todo el día y, simplemente, la dejo funcionar», señala Kraft. «No tengo que estar pegado a la pantalla y de un vistazo puedo ver la información que necesito».

Con la consola de administración de Malwarebytes, Kraft puede administrar de forma rápida y sencilla el software de Malwarebytes en los clientes mientras evalúa la seguridad general de los terminales de la empresa, y todo desde una sola pantalla. Puede ordenar por Últimas amenazas detectadas e identificar rápidamente cualquier anomalía. Sabe de inmediato cuándo se está realizando un análisis y obtiene resultados un 50 por ciento más rápido que con su anterior solución antivirus.

«Sé que Malwarebytes permite ahorrar tiempo y que los equipos de nuestros empleados funcionan mejor», asegura Kraft. «Vermeer ha dado los pasos correctos e implementado los procedimientos recomendados para proteger a los usuarios de los terminales».

## | Acerca de

Malwarebytes ofrece soluciones de software anti-malware y anti-exploit diseñadas para proteger a empresas y usuarios frente a las amenazas de día cero que continuamente escapan a la detección de los antivirus tradicionales. Malwarebytes Anti-Malware obtuvo una calificación de Sobresaliente otorgada por los editores de CNET, es el programa favorito de los editores de PCMag.com y fue el único software de seguridad que obtuvo una puntuación perfecta en desinfección de malware según AV-TEST.org. Ese es el motivo por el que más de 38 000 PYMES y empresas globales confían en Malwarebytes para proteger los datos. Fundada en 2008, Malwarebytes tiene su sede principal en California, mantiene varias oficinas en Europa y emplea a un equipo global de investigadores y expertos.



Santa Clara, CA



malwarebytes.com



corporate-sales@malwarebytes.com



1.800.520.2796