Malwarebytes

CASO PRÁCTICO

Faith Regional Health Services se vacuna frente al malware

Un proveedor de atención sanitaria bloquea el paso al malware y los exploits con Malwarebytes Endpoint Security

SECTOR
Sanidad

DESAFÍO COMERCIAL
Detener una avalancha de malware que impedía a los técnicos dedicar más tiempo a proyectos útiles que mejoraran la calidad de la atención al paciente.

ENTORNO DE TI
Un centro de datos con Microsoft Security Central y Check Point 4800 Appliance con firewall, Sophos AV, control de aplicaciones, red privada virtual (VPN) y sistema de prevención de intrusiones (IPS)

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

RESULTADOS
- Reducción de las amenazas de varios miles a ninguna
- Horas y días ahorrados en tiempo de los técnicos dedicados a desinfectar los equipos
- Mayor satisfacción de los usuarios en cuanto a rendimiento de los PC
- Solución más sencilla para preservar la conformidad con las normas HIPAA y PCI DSS

Perfil de la empresa

Faith Regional Health Services ha proporcionado atención sanitaria a los residentes de la zona noreste de Nebraska desde 1923. En la actualidad, atiende a una población de 156 000 personas en 13 condados, proporcionando asistencia médica mediante un hospital de 200 camas, 20 clínicas y 12 ubicaciones remotas. Cuando se produjo una epidemia de malware, Faith Regional pidió ayuda a Malwarebytes para remediarla.

> El malware estaba a nuestro alrededor y era un gran quebradero de cabeza a la hora de preservar la normativa de la HIPAA y el PCI DSS. Ahora estamos tranquilos porque el malware ni siquiera llega a entrar.
>
> —Paul Feilmeier, director de infraestructuras de TI, Faith Regional Health Services

Desafío comercial

Ponga freno a los frustrantes ataques de malware

Una creciente oleada de malware estaba causando estragos en el servicio técnico del Faith Regional y en sus equipos de técnicos de campo. Estábamos desbordados por los más de 20 o 30 equipos a la semana que necesitaban limpieza o restauración debido al malware y la situación se volvió frustrante para todos, técnicos, empleados de la oficina y médicos.

Los empleados perdieron un tiempo muy valioso mientras se desinfectaban los equipos. Para los médicos, el tiempo de inactividad obligó a interrumpir la atención sanitaria a los pacientes. Aunque los técnicos proporcionaran equipos de sustitución, se tenían que configurar los nuevos terminales e instalar en ellos las aplicaciones básicas y darles acceso a la red. Cuando se detectaban PC infectados en una de las clínicas, un miembro del equipo técnico tenía que desplazarse hasta allí para desinfectarlos. Eso significaba perder un día entero solo para limpiar un equipo.

El Malware, al igual que los bots y cualquier otra amenaza de comando y control, puede comprometer la privacidad de los datos a través de los terminales y poner en peligro el cumplimiento de la HIPAA y el PCI DSS.

Con decenas de medidas en marcha para garantizar que Faith Regional cumpliera con los requisitos de dichas normas, lo último que necesitaba el equipo de TI era una preocupación más.

«Necesitábamos una forma mejor de luchar contra la creciente oleada de malware y bots», afirma Paul Feilmeier, director de infraestructuras de TI en Faith Regional Health Services. «Nuestra solución antivirus, Sophos, eliminaba los virus pero era incapaz de eliminar el malware de forma efectiva». El equipo de TI empezó a evaluar las opciones de lucha contra el malware y eligieron Malwarebytes Endpoint Security.

La solución

Malwarebytes Endpoint Security

Malwarebytes Endpoint Security ofrece una potente defensa en varias capas diseñada para eliminar el malware más reciente y peligroso, incluido el ransomware. Incluye Malwarebytes Anti-Malware, Anti-Exploit, y la consola de administración en una completa solución. El administrador del sistema de Faith Regional implementó Malwarebytes en los terminales y en los servidores, y a los dos días ya estaba generando los primeros informes.

El antídoto para el malware

«Después de implementar Malwarebytes, los informes que proporcionaba eran asombrosos», afirma Feilmeier. «Había miles de archivos infectados en los equipos. Nuestros usuarios estaban completamente frustrados con los efectos de tal avalancha de malware».

Malwarebytes destapó decenas de programas potencialmente no deseados (PUP, por sus siglas en inglés) y de modificaciones potencialmente no deseadas (PUM). Bloqueó el acceso a numerosos sitios web maliciosos. Y Malwarebytes Anti-Exploit defendió satisfactoriamente los equipos frente a los exploits, incluido el heap spraying, las descargas de archivos maliciosos, los exploits de Java, los ataques a la programación orientada al retorno y los intentos de burlar la protección de ASLR. Las amenazas detectadas diariamente cayeron de 1800 a cero.

«La consola de administración también mostraba qué grupos de usuarios tenían constantemente problemas con el malware», comenta. «Esto nos permitía proporcionar una mejor formación acerca de las amenazas en línea y los elementos en los que nunca se debe hacer clic».

Permite mantener un entorno seguro y conforme a las normas

Gracias a Malwarebytes, Faith Regional consiguió detener el malware e incluso prevenirlo. El software actualiza de forma activa las definiciones y supervisa los terminales y los servidores prácticamente sin ninguna intervención por parte de los técnicos. Si los técnicos detectaban alguna actividad sospechosa en la red, avisaban a los miembros del equipo. Ellos podían analizar y limpiar de malware los equipos de forma remota. El usuario no lo notaba y la productividad no caía.

«El malware estaba a nuestro alrededor y era un gran quebradero de cabeza a la hora de preservar la normativa de la HIPAA y el PCI DSS», asegura Feilmeier. «Ahora estamos tranquilos porque el malware ni siquiera llega a entrar».

Pudieron volver a centrarse en aquellos proyectos que mejoran la atención del paciente

Los técnicos aseguraron rotundamente que Malwarebytes constituye una gran inversión y que disfrutan de sus ventajas a diario. Gracias al programa, han recuperado tiempo para concentrarse en nuevos proyectos en lugar de en administrar incidencias técnicas. En la actualidad, los miembros del soporte técnico y los técnicos de campo disponen de más tiempo para colaborar con el personal sanitario para implementar nuevas aplicaciones y funcionalidades en todos los hospitales y clínicas.

«A menudo, nuestros usuarios no comprenden la importancia de las TI en la atención sanitaria», asegura Feilmeier. «Pero cuando los PC funcionan correctamente y de forma estable, los médicos no están frustrados. Todo funciona con más normalidad. Y todo ello contribuye a mejorar la experiencia del paciente y la atención sanitaria».

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