Malwarebytes

ÉTUDE DE CAS

Faith Regional Health Services se protège contre les programmes malveillants

Un prestataire de soins de santé bloque les malwares et les exploits grâce à Malwarebytes Endpoint Security.

SECTEUR
Santé

ENJEU POUR L'ENTREPRISE
Endiguer une épidémie de malwares qui a détourné les techniciens de projets visant à améliorer les soins prodigués aux patients

ENVIRONNEMENT INFORMATIQUE
Un centre de données avec Microsoft Security Central et appliance Check Point 4800 avec pare-feu, Sophos AV, contrôle des applications, réseau privé virtuel (RPV) et système de prévention d'intrusions (IPS)

SOLUTION
Malwarebytes Endpoint Security, qui inclut Anti-Malware, Anti-Exploit et la console de gestion

RÉSULTATS
- Passage de milliers de menaces à zéro menace
- Pour les techniciens, une économie en temps de dépannage qui se compte en jours entiers
- Plus grande satisfaction des utilisateurs du fait d'ordinateurs plus performants
- Maintien aisé de la conformité aux normes HIPAA et PCI DSS

Profil commercial

Faith Regional Health Services fournit des soins de santé aux résidents du nord-est du Nebraska depuis 1923. Le groupe dessert aujourd'hui une population de 156 000 personnes réparties dans 13 comtés, en offrant des services médicaux grâce à un hôpital de 200 lits, 20 cliniques et 12 sites éloignés. Lorsqu'une épidémie de programmes malveillants l'a frappé, Faith Regional s'est adressé à Malwarebytes.

> Notre environnement était truffé de malwares et nous étions très inquiets quant à la conformité avec les normes HIPAA et PCI DSS. À présent, nous avons la certitude que les malwares n'atteignent même pas notre système.
>
> —Paul Feilmeier, responsable de l'infrastructure informatique, Faith Regional Health Services

Enjeu pour l'entreprise

Endiguer le flux de malwares frustrants et dérangeants

Une avalanche de malwares a fait des ravages au centre d'assistance et chez les techniciens de terrain de Faith Regional. Nous croulions sous les ordinateurs infectés. Toutes les semaines, 20 à 30 PC devaient être nettoyés ou reformatés à cause de programmes malveillants. Techniciens, employés de bureau et personnel médical, nous étions tous frustrés.

Les employés ont perdu un temps précieux pendant le nettoyage de leurs machines. Pour les médecins, cette indisponibilité était frustrante et a interrompu les soins des patients. Même lorsque le service informatique fournissait une machine de remplacement, il était nécessaire de configurer, installer les applications de base et établir un accès réseau sur le nouveau matériel. Lorsque les PC infectés étaient situés dans une clinique, un membre de l'équipe informatique devait se rendre sur place pour dépanner la machine. Nous pouvions perdre une journée entière pour nettoyer une seule machine.

Les malwares, tels que les bots et autres menaces de prise de contrôle, pouvaient également compromettre les données grâce à des dispositifs terminaux ainsi que la conformité aux normes HIPAA et PCI DSS. Avec les dizaines de contrôles mis en place pour garantir la conformité de Faith Regional avec ces normes, l'équipe informatique n'avait pas besoin de ce souci supplémentaire.

« Nous devions trouver un meilleur moyen de combattre ce flux incessant de malwares et de bots », explique Paul Feilmeier, responsable de l'infrastructure informatique chez Faith Regional Health Services. « Notre antivirus Sophos détectait les virus, mais ne détectait pas efficacement les malwares. » L'équipe informatique a commencé à évaluer les options à sa disposition pour combattre les malwares et a choisi Malwarebytes Endpoint Security.

La solution

Malwarebytes Endpoint Security

Malwarebytes Endpoint Security protège les terminaux grâce à une défense multicouche conçue pour éliminer les malwares les plus récents et les plus dangereux, y compris les ransomwares. Cette solution inclut dans une solution complète Malwarebytes Anti-Malware, Anti-Exploit et la console de gestion. L'administrateur système de Faith Regional a déployé Malwarebytes sur les terminaux et les serveurs et a obtenu ses premiers rapports en deux jours seulement.

L'antidote aux malwares

« Les rapports obtenus juste après le déploiement de Malwarebytes étaient on ne peut plus éloquents », déclare Paul Feilmeier. « Les machines comportaient des milliers de fichiers infectés. Nos utilisateurs devaient être extrêmement frustrés par les effets de tant de malwares. »

Malwarebytes a détecté des dizaines de programmes potentiellement indésirables (PUP) et de modifications potentiellement indésirables (PUM). Il a bloqué l'accès à de nombreux sites Web malveillants. Malwarebytes Anti-Exploit a également défendu avec succès des machines contre les exploits, notamment la pulvérisation sur le tas, le téléchargement de codes malveillants, les exploits Java, les attaques de programmation orientée retour et les tentatives de contournement ASLR. Les détections de menaces quotidiennes sont passées de 1 800 à zéro.

« La console de gestion a indiqué les groupes d'utilisateurs qui avaient en permanence des problèmes avec les malwares », poursuit-il. « Cela nous permet de mieux former notre personnel sur les menaces en ligne, et sur les éléments sur lesquels il ne faut pas cliquer. »

Maintenir de bons signes vitaux et préserver la conformité légale

Avec Malwarebytes, Faith Regional a pu éloigner durablement les malwares. Le logiciel met activement à jour les définitions et surveille les terminaux et serveurs, et nécessite peu ou pas d'intervention de la part des techniciens. Si les techniciens réseau constatent une activité suspecte sur le réseau, ils alertent l'équipe de bureau. Ceux-ci peuvent analyser la machine à distance et supprimer les malwares. L'opération est totalement transparente pour l'utilisateur, dont la productivité n'est pas affectée.

« Notre environnement était truffé de malwares, et nous étions très inquiets quant à la conformité avec les normes HIPAA et PCI DSS », indique Paul Feilmeier. « À présent, nous avons la certitude que les malwares n'atteignent même pas notre système. »

Remettre l'accent sur les projets synonymes d'une plus grande qualité de soins

Les techniciens sont unanimes, Malwarebytes est un très bon investissement et ils en constatent les bénéfices chaque jour. Ils gagnent du temps et peuvent ainsi se concentrer sur leurs projets, au lieu de résoudre des problèmes. À présent, le centre d'assistance et les équipes de terrain passent davantage de temps avec le personnel soignant pour développer de manière proactive de nouvelles applications et capacités, pour l'hôpital ainsi que les cliniques.

« Bien souvent, nos utilisateurs ne réalisent pas l'impact de l'informatique sur les soins prodigués aux patients », déclare Paul Feilmeier. « Mais quand les ordinateurs sont stables et fonctionnent, les médecins ne sont pas frustrés. Tout fonctionne mieux. Et tout cela contribue à une meilleure expérience des patients et à de meilleurs soins. »

À propos

Malwarebytes fournit des logiciels anti-malware et anti-exploit conçus pour protéger les entreprises et les consommateurs contre les menaces zero day que les antivirus traditionnels ne sont pas capables de détecter. Malwarebytes Anti-Malware a reçu la mention « remarquable » de la part des éditeurs de CNET et fait partie des recommandations des éditeurs de PCMag.com. Il est aussi le seul logiciel de sécurité à avoir obtenu un score parfait en matière de suppression des malwares lors d'essais menés par AV-TEST.org. C'est pourquoi plus de 38 000 PME et grandes entreprises du monde entier font confiance à Malwarebytes pour protéger leurs données. Fondée en 2008 et basée en Californie, Malwarebytes possède des bureaux en Europe et emploie une équipe internationale de chercheurs et d'experts.

Santa Clara, Californie

malwarebytes.com

corporate-sales@malwarebytes.com

1.800.520.2796