Faith Regional Health Services inoculates itself against malware

Healthcare provider blocks malware and exploits with Malwarebytes Endpoint Security

INDUSTRY
Healthcare

BUSINESS CHALLENGE
Stop an epidemic of malware that stole technicians' time from proactive projects that improve patient care

IT ENVIRONMENT
One data center with Microsoft Security Central and Check Point 4800 Appliance with firewall, Sophos AV, app control, Virtual Private Network (VPN), and Intrusion Prevention System (IPS)

SOLUTION
Malwarebytes Endpoint Security, which includes Anti-Malware, Anti-Exploit, and the Management Console

RESULTS
- Reduced threats from thousands to zero
- Saved hours and days of technicians' time from remediating machines
- Improved user satisfaction with PC performance
- Simplified the ability to maintain HIPAA and PCI DSS compliance

Business profile

Faith Regional Health Services has delivered healthcare to the residents of northeast Nebraska since 1923. Today, it serves a population of 156,000 people across 13 counties, providing medical services through a 200-bed hospital, at 20 clinics, and in 12 remote locations. When a malware epidemic hit, Faith Regional turned to Malwarebytes for the cure.

> Malware was in our environment and that was a huge source of concern when it comes to maintaining HIPAA and PCI DSS compliance. Now we're sure that malware doesn't even get in to start with.
>
> —Paul Feilmeier, IT Infrastructure Manager, Faith Regional Health Services

Business challenge
Stem the tide of frustrating, disruptive malware

A growing flood of malware was wreaking havoc on Faith Regional's help desk and field technician teams. Inundated by 20 to 30 PCs a week that required cleaning or re-imaging due to malware, the situation was frustrating for everyone—technicians, business office employees, and clinicians.

Employees lost valuable time while machines were being remediated. For clinicians, downtime was frustrating and interrupted patient care activities. Even when IT could provide a replacement machine, the new endpoint still had to be configured and installed with basic applications and network access. When infected PCs were located at a clinic, an IT team member would have to travel to the site to remediate them. That could mean losing an entire day to clean just one machine.

Malware, such as bots and other command-and-control threats, also could compromise data through endpoint devices and
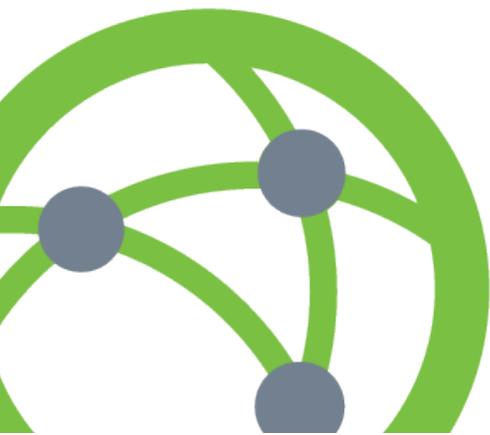
jeopardize HIPAA and PCI DSS compliance. With dozens of controls in place to help ensure that Faith Regional meets the requirements of those standards, the IT team didn't need one more worry.

"We needed a better way to fight an ever-growing flood of malware and bots," said Paul Feilmeier, IT Infrastructure Manager at Faith Regional Health Services. "Our Sophos antivirus solution caught viruses, but it wasn't catching malware effectively." The IT team began evaluating their options for fighting malware and chose Malwarebytes Endpoint Security.

The solution

Malwarebytes Endpoint Security

Malwarebytes Endpoint Security provides a powerful multi-layered defense engineered to defeat the latest, most dangerous malware, including ransomware. It includes Malwarebytes Anti-Malware, Anti-Exploit, and the Management Console in one comprehensive solution. Faith Regional's system administrator deployed Malwarebytes on endpoints and on servers and was generating its first reports in just two days.

The antidote to malware

"After we deployed Malwarebytes, the reports it delivered were amazing," said Feilmeier. "There were thousands of infected files on machines. Our users had to have been extremely frustrated with the effects of so much malware."

Malwarebytes uncovered dozens of different Potentially Unwanted Programs (PUPs) and Potentially Unwanted Modifications (PUMs). It blocked access to numerous malicious websites. And Malwarebytes Anti-Exploit successfully defended machines against exploits including heap spraying, malicious payload downloads, Java exploits, return-oriented programming attacks, and ASLR bypass attempts. Daily threat detections dropped from 1,800 to zero.

"The management console also showed which groups of users continually had problems with malware," he said. "That enabled us to provide better education about online threats and what not to click on."

Maintains healthy vital signs and compliance

With Malwarebytes, Faith Regional was able to get—and stay—ahead of malware. The software actively updates definitions and monitors endpoints and servers with little or no intervention from technicians. If the network technician notices suspicious network activity, he alerts the desktop team. They can remotely scan the machine and clean it of malware. The user never notices, and productivity doesn't suffer.

"Malware was in our environment and that was a huge source of concern when it comes to maintaining HIPAA and PCI DSS compliance," said Feilmeier. "Now we're sure that malware doesn't even get in to start with."

Refocused on projects that improve patient care

The technicians emphatically declared that Malwarebytes is a great investment—and they experience its benefits every day. They've regained time to focus on projects instead of trouble tickets. Now, help desk and field team members spend more time with healthcare staff to proactively deploy new applications and capabilities throughout the hospital and clinics.

"Often, our users don't realize the impact of IT on patient care," said Feilmeier. "But when PCs are stable and running, clinicians aren't frustrated. Everything operates more smoothly. And it all contributes to a better patient experience and better patient care."