CASE STUDY

School district stays clear of ransomware

Malwarebytes restores confidence against ransomware attacks

Business profile

The historic town of Bloomsburg, PA is the portrait of small-town America. With 14,000 residents, the Bloomsburg Area School District educates 1,600 students from kindergarten through Grade 12. Despite the fact that the district is small and semi-rural, it suffered a ransomware attack. But only one. After the district deployed Malwarebytes, ransomware is nowhere to be found.

Business challenge

Prevent ransomware from returning

With 200 teachers and administrators plus 1,600 students, the IT team of four has its hands full. They're responsible for the desktop, lab PCs, and tablets at six locations, as well as all of the network and communications technology for the district. Even one malware incident takes valuable time away from keeping everything up and running. When ransomware hit, it took more than two days to get things back to normal.

"A teacher accidentally downloaded a file that included ransomware," said Gary Honabach, Technology Systems Administrator for Bloomsburg Area School District. "By the time we identified it, the teacher's machine was compromised and so were network files that she had accessed. It took us at least 16 hours to get back to a situation where shared files were safe to use again. We decided we needed more protection."

The solution

Malwarebytes Endpoint Security

The team first looked online for solutions that prevent ransomware and malware. After evaluating several options and reading white papers, Honabach and his team decided to try Malwarebytes. Several team members had previous experience with Malwarebytes, and they initiated a test.

OVERVIEW

INDUSTRY
Education

BUSINESS CHALLENGE
Prevent ransomware attacks from affecting students and staff

IT ENVIRONMENT
Microsoft System Center Endpoint Protection for antivirus, email spam filtering, SonicWALL firewall, content filtering

SOLUTION
Malwarebytes Endpoint Security

RESULTS
Stopped ransomware from returning and infecting machines

Deployed quickly and easily in the background, requiring minimal staff time

Significantly reduced the need to reimage infected machines

Delivered security, knowing that threats are proactively blocked

“We started with five machines, installed Malwarebytes, and they worked flawlessly,” said Honabach. “That—plus our previous experience—made us confident to move forward. We currently have about 800 machines protected with Malwarebytes.”

The district deployed Malwarebytes Endpoint Security for its teachers, staff, and high school endpoints, which are Microsoft Surface Pro systems used for a one-to-one computing initiative. In less than two months all of the systems were deployed and ready to go when the new school year started.

We did it ourselves

Honabach says that his technicians are savvy and they had no issue deploying Malwarebytes whatsoever. Over summer breaks, the team collects all of the student machines, inspects them, cleans them up, and then installs any new software updates. Bloomsburg created a deployment package through Microsoft System Center Configuration Manager and automatically pushed out Malwarebytes.

“We just put machines up on the rack, turned them on, and deployed Malwarebytes in the background,” said Honabach. “The next time the student uses the computer, new software and Malwarebytes are there. It’s seamless.”

Minds at ease

Since Malwarebytes was deployed, Honabach says that they haven’t experienced any more issues with ransomware. If a machine gets a toolbar or other type of malware, Malwarebytes automatically takes care of it. The number of malware incidents has dramatically diminished.

“Malwarebytes gives us the security of knowing that malware and ransomware will be quarantined before infecting a user’s device,” said Honabach, “keeping machines from being compromised.”

In the past, the team spent hours every week cleaning off popup windows and other malware from elementary and high school student machines. Even though it wasn’t difficult to reimage machines, it took staff time to get the machine to the lab and initiate the reimaging process. Not only that, the student would be without a computer for one to two days.

Does the heavy lifting

With so few staff supporting 800 devices and the entire network, Malwarebytes does a lot of heavy lifting for the district. Immediately after deployment, the team received numerous notifications for several months until machines had been cleaned off. Now, Honabach can go about his other work knowing that Malwarebytes has his back. If anything is identified on a machine, he receives an email notification and knows exactly what is occurring.

“I haven’t had a notification in at the past several months,” he said. “We wanted something that would run by itself, and it does. Everything just clicks.”

> “
>
> MALWAREBYTES GIVES US THE SECURITY OFKNOWING THAT MALWARE AND RANSOMWARE WILL BE QUARANTINED BEFORE INFECTING A USER’S DEVICE, KEEPING MACHINES FROM BEING COMPROMISED.
>
> GARY HONABACH, TECHNOLOGY SYSTEMS ADMINISTRATOR, BLOOMSBURG AREA SCHOOL DISTRICT

Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware and exploits that escape detection by traditional antivirus solutions. Malwarebytes completely replaces antivirus with artificial intelligence-powered technology that stops cyberattacks before they can compromise home computers and business endpoints. Learn more at www.malwarebytes.com.