Malwarebytes

CASE STUDY

Betty Hardwick Center elevates endpoint security to a new level

Malwarebytes finds everything that other solutions missed

INDUSTRY
Healthcare

BUSINESS CHALLENGE
Eliminate system performance problems and user downtime due to malware

IT ENVIRONMENT
Antivirus, firewalls

SOLUTION
Malwarebytes Endpoint Security, Premium Service

RESULTS

- Reduced malware infections to nearly zero and prevented ransomware infections
- Eliminated persistent computer performance issues due to malware
- Gained ability to easily manage and remediate systems remotely

Business profile

The Betty Hardwick Center is the Mental Health and Intellectual and Developmental Disability Authority for five counties surrounding Abilene, Texas. The center began serving clients in 1971 with the mission of improving the behavioral, intellectual, and developmental health of the people it serves. The team decided to take no chances in protecting the health of its computers and deployed Malwarebytes.

> We tested a number of solutions. We'd have a system running as slow as molasses, and the antivirus solution would scan it and find nothing. With Malwarebytes we'd get multiple hits almost instantly.
>
> —John Cizek, Network and Telecommunications Administrator, Betty Hardwick Center

Business challenge

Ramping up protection

Staff members at the Betty Hardwick Center work with children, adolescents, and adults who have mental health issues or intellectual and developmental disabilities. They visit clients in their homes to follow up on doctor visits, review treatment plans, help with housing and educational opportunities, and make sure that they are receiving the services they need.

Employees in the field carry laptops to log into the center's network over the Internet. While mobile, these systems are more exposed to potential malware attacks than the onsite computers. Onsite desktop computers are protected with antivirus solutions, firewalls, and other security measures. Even though antivirus solutions run on all systems, the IT team began to see a growing number of malware infections that the antivirus products missed.

"We have had several antivirus solutions that are supposed to protect our endpoints," said John Cizek, Network and Telecommunications Administrator for the Betty Hardwick Center. "We found that although they advertised protection against malware, they didn't do it very well. Viruses, yes. Malware, no."

The threat of ransomware made it more urgent to find a new solution. Although the Betty Hardwick Center had not experienced a ransomware attack, similar centers in the state had. The attacks crippled operations for several weeks and cost tens of thousands of dollars to remediate and recover.

The solution

Malwarebytes Endpoint Security

In the past, Cizek's team used Malwarebytes to clean the occasional malware infection. As infections became more frequent, they tested a number of solutions to stop them. When the team learned about Malwarebytes Endpoint Security, everything changed.

"We tested a number of solutions," said Cizek. We'd have a system running as slow as molasses, and the antivirus solution would scan it and find nothing. With Malwarebytes we'd get multiple hits almost instantly."

The center purchased Malwarebytes and deployed it across all desktops and laptops. The Management Console made it easy to push the software out and within a few days, the malware count had dropped dramatically.

"I was elated," said Cizek. "Now we could be proactive in stopping malware and ransomware—instead of reactive—and that changed a whole lot."

Redefining "clean"

Cizek says that peace of mind is the biggest benefit. When Malwarebytes runs and says a machine is clean, it's clean. For example, one of the center's executives reported that her system was extremely slow. Opening an email or Word document took minutes, and she couldn't access the Internet. The team ran two antivirus programs and a disk-clean utility looking for damaged sectors on the hard drive. Everything came up fine, but the machine still ran slowly.

"I just didn't buy it," said Cizek. "I knew there was something there. We scanned it with Malwarebytes and found 429 different pieces of malware on it. What other products don't catch, Malwarebytes does."

Proactive protection

Malwarebytes web protection keeps users from going to suspicious or infected sites. If a user tries to visit a potentially dangerous site, it notifies the user that the site might be compromised. If the user decides to go anyway, Malwarebytes will stop them if it detects malicious content. Many times, Malwarebytes has detected exploits on popular sites, such as MSN, or on sites that are connected directly with the state. When it does, Cizek will notify the state or the agency that owns the infected site.

"A lot of times, they'll say 'thanks for notifying us, but we don't see a problem'," said Cizek. "Sure enough, about a week later, we'll get an alert to batten down the hatches because of it. They could have avoided the whole problem by using Malwarebytes."

Nothing escapes

The Management Console makes it simple to see endpoints that aren't protected or need updating. Malwarebytes has detected and stopped a wide range of malware threats at the center—Trojans, doomsday worms, and zero-day variants. If Malwarebytes alerts the team to a potential issue, they can actually see the user's screen and take action remotely. If they can't clear the problem remotely, they will isolate the system and inspect it physically.

"Malwarebytes backup support is a huge help," said Cizek. "If the product detects something new, it puts it in quarantine, or timeout, as I call it. We connect to Malwarebytes support in a remote session, and they'll have a knockdown drag-out fight with it to find it, identify it, and fix it. That's the cool thing about Malwarebytes. It catches malware that none of the other products catch."

About

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.

Santa Clara, CA

malwarebytes.com

corporate-sales@malwarebytes.com

1.800.520.2796