

San Jacinto USD closes the book on ransomware

Prevents ransomware and malware from gaining access to students, teachers, and staff

INDUSTRY
Education

BUSINESS CHALLENGE
Prevent ransomware from affecting teaching and learning

IT ENVIRONMENT
Sophos antivirus

SOLUTION
Malwarebytes Endpoint Security

RESULTS

- Saved at least \$1,000 per week in labor costs from remediating malware
- Simplified management with continuous visibility into endpoints
- Allowed IT team to focus on advancing classroom technology instead of fighting malware

Business profile

The San Jacinto Unified School District (USD) of Riverside County, California, serves 9,800 students in seven elementary schools, three middle schools, and three high schools. The district also operates preschool and community-based adult transition programs. With a staff of 1,000 and additional student computers, the flood of ransomware on the Internet was bound to affect the district. San Jacinto USD chose Malwarebytes to stop ransomware from stealing time from its IT team and teachers.



In the past, we easily spent 10 hours a week cleaning up malware. With Malwarebytes handling prevention, detection, and remediation, we save at least \$1,000 per week in labor costs during the school year.

—Chawn Lytle, Director of Technology Services,
San Jacinto Unified School District

Business challenge

Stopping ransomware from affecting productivity

The district has almost 3,000 Microsoft Windows PCs, as well as Google Chromebooks. Although the Sophos antivirus solution was catching viruses, advanced threats like exploits and ransomware were getting through. Whether staff machines were infected via drive-by attacks on their browsers or a user accidentally clicking on a malicious link, the result was the same. Web browsers were hijacked, pop-ups proliferated, and ransomware found its way in.

“When ransomware got through, it spread to shared network drives that the user had permissions to,” said Dave Baker, Technology Support Specialist for the San Jacinto Unified School District. “We could recover from it, but remediation was time-consuming.”

Each time a computer became infected with ransomware, it took several hours to remove it. At least a full day each week was spent on containing ransomware and re-imaging machines from backup. And that didn’t even include addressing calls from users who were experiencing dozens of pop-ups and attempts to hijack their browsers.



The solution

Malwarebytes Endpoint Security

The district's primary requirement was to block ransomware, but it also wanted real-time malware prevention, detection, and remediation to increase security and uptime. Baker had used Malwarebytes effectively at another business and recommended it to the school district.

"We piloted a program at San Jacinto USD using Malwarebytes on a computer lab, and the team purposely went to known malicious sites," said Baker. "Malwarebytes caught every one of them."

Malwarebytes also helped the district set up its Malwarebytes Management Console. The Management Console made it easy to push the Malwarebytes software to more than 2,000 Windows PCs.

Seeing the big picture

"Before Malwarebytes, we might see an alert in our antivirus console," said Baker, "but that was a small percentage of what was really out there. Usually, we wouldn't know that there was a problem until end users called because their browsers were acting up or their files were suddenly encrypted."

Now Baker can scan the network and immediately see any unprotected computers. He also retrieves reports of malware and exploits that have been blocked.

"At a glance, I see that there were more than 36,000 threats in the past month," he said. "Malwarebytes notified us of Potentially Unwanted Programs (PUPs), Potentially Unwanted Modifications (PUMs), and other threats, and we have not had any more ransomware issues."

Simplifying management

San Jacinto USD uses the Malwarebytes Management Console to ensure that all endpoints are protected

and easily updated. It integrated the Malwarebytes Management Console with Active Directory, enabling the team to simplify management with visibility into all of the endpoints in their specific organizational units.

"We also purchased Malwarebytes support, and it's well worth it," said Baker. "Malwarebytes is very responsive and helpful. I rarely have to call, but when I do, we resolve the issue quickly. That's a lot of peace of mind right there."

Saving time and re-focusing resources

With only seven IT staff to support the entire district, malware and ransomware had a huge impact on productivity. It consumed field technicians' time and swamped the help desk with phone calls, and the systems manager had to clean up the endpoints.

"In the past, we easily spent 10 hours a week cleaning up malware," said Chawn Lytle, Director of Technology Services for San Jacinto USD. "With Malwarebytes handling prevention, detection, and remediation, we save at least \$1,000 per week in labor costs during the school year."

Now the tech team can proactively visit each school and go classroom to classroom, talking with teachers to identify any computer or network issues and help them maximize use of their classroom technology. They have also conducted in-service sessions that taught staff how to identify potentially malicious emails and links. Schools also teach "web etiquette" to students, helping them to better understand the risks of visiting potentially malicious sites.

"We're able to move forward on more projects that advance education," said Baker. "Just knowing that Malwarebytes is doing its job allows us to focus our attention on other areas that better serve the district."

| 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