

At Colorado Springs School District 11, nothing holds students back—especially not malware

School effectively protects 17,000 endpoints from CryptoWall and other malware

INDUSTRY
Education

BUSINESS CHALLENGE
Prevent disruption to teaching and learning because of malware-related problems

IT ENVIRONMENT
One data center with Cisco firewall, intrusion prevention, FireEye Enterprise Network Security, and Microsoft System Center Endpoint Protection antivirus

SOLUTION
Malwarebytes Anti-Malware for Business, which includes the Management Console

RESULTS

- Help stop CryptoWall attacks from re-occurring
- Remediated malware across the district and reduced infected machines from dozens to virtually none
- Saved hundreds of hours of time and associated cost
- Drove proactive policies for better endpoint protection

Business profile

Colorado Springs School District 11 offers parents and students a wide range of individualized programs in its elementary, middle, and high schools. Just one IT center and a lean staff support 17,000 endpoints for teachers, staff, and students across 60 schools and operations facilities. The IT team also supports classroom technology such as desktops, laptops, smart boards, tablets, printers, and applications. That's a lot to manage, and malware incidents can quickly derail IT productivity and grind classroom learning to a halt.



Malwarebytes has saved us hundreds of hours otherwise spent remediating systems. This translates to significant cost savings and allows technicians to focus on more productive projects.

—Dan Boltjes, Director of Technical Services,
Colorado Springs School District 11

Business challenge

Prevent classroom downtime

The district's antivirus solution was identifying traditional viruses, but malware continued to get through and proliferate. A growing number of Potentially Unwanted Programs (PUPs), redirects, and toolbars escaped notice by the antivirus solution. Students' machines had a high number of botnet infections, often introduced through external USB drives. Staff machines tended to experience social engineering types of attacks. In both cases, performance slowed or malware disrupted the machine's functionality. If a school's library technology



technician could not fix the problem, a field technician was dispatched to the location.

Re-imaging the machines was usually the fastest way to remediate the malware and get the user back online. However, with multiple malware issues and only five field technicians between 60 locations, remediating malware was consuming an unacceptable amount of technicians' time.

The final straw arrived in the form of a CryptoWall attack. CryptoWall heavily affected one school, as well as several departments in the district's central administration complex. Although the infection was cleaned up, it was obvious that the district was not immune.

"A CryptoWall attack can cause significant teaching and learning disruption across our district," said Dan Boltjes, Director of Technical Services at Colorado Springs School District 11. "An attack like that leaves you wondering when the next shoe will drop and how far it will proliferate. We decided to add another layer to our endpoint protection scheme."

The solution

Malwarebytes Anti-Malware for Business

"We tested several solutions before narrowing our final selection to Malwarebytes," said William Fisher, Senior TOSS at Colorado Springs School District 11. "I'd heard good things about Malwarebytes from our field and library technology technicians. After the evaluation, Malwarebytes was indeed the best alternative for us."

The IT team initially deployed Malwarebytes Anti-Malware for Business on 350 machines in mission-critical departments, such as payroll, business services, Human Resources, and IT. After the initial deployment, the

machines remained free from malware, and the team began pushing Malwarebytes to all 17,000 endpoints.

Automatic scans and daily updates

Today, Malwarebytes scans machines weekly, although Fisher checks endpoints daily through the Malwarebytes Management Console. Machines are updated as needed and stay current.

"Malwarebytes Anti-Malware for Business really cleaned things up for us," said Fisher. "Before, we saw many botnet infections, and now we see far less of that activity."

Nor has the district experienced any further widespread CryptoWall attacks. The Malwarebytes anti-malware proactive heuristic scanning engine can identify and block attacks like CryptoWall in addition to blocking user access to malicious websites. These capabilities have dramatically reduced the district's exposure to malware.

Hundreds of hours saved

According to Fisher, the district has nowhere near the issues that it had prior to deploying Malwarebytes. Library technology and field technicians no longer have to spend hours tracking down a malware-related problem or re-imaging machines. Malwarebytes removed much of that frustration.

"Malwarebytes has saved us hundreds of hours otherwise spent remediating systems," said Boltjes. "It translates to significant cost savings too, because technicians can focus on more productive projects."

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