

Klamath-Trinity Joint Unified School District marks malware “absent”

The school district uses Malwarebytes Anti-Malware for Business to find and eliminate malware on teachers’ workstations

INDUSTRY

Education

BUSINESS CHALLENGE

Stopping Trojans and securing endpoints

IT ENVIRONMENT

The school district deployed content filters, Cisco ASA firewalls, and AVG antivirus software

SOLUTION

750 licenses of Malwarebytes Anti-Malware for Business, which includes the Management Console

RESULTS

- Simplified and accelerated deployment
- Eliminated hours of time spent cleaning machines
- Gained visibility and ability to proactively address threats

Business profile

The Klamath-Trinity Joint Unified School District encompasses eight schools and 1,200 students in Humboldt County, California. Although the district had antivirus software installed on approximately 175 endpoints, it was not keeping up with malware. And because of budget constraints, those endpoints were only a portion of the district’s total inventory of 670 computers in stationary and mobile labs, as well as on teachers’ desks.



Malwarebytes gives us a tremendous comfort level. We don’t have to constantly worry about threats. Now we have the tool we need to move forward to 1:1 computing with confidence.

—David Elie, District Technician, Klamath-Trinity Joint Unified School District

Business challenge

Stopping Trojans and securing endpoints

“We knew that a growing number of Trojans were infecting teachers’ workstations,” said David Elie, District Technician for the school district. “Our existing antivirus solution wasn’t catching them and they would bring systems down completely.”

Worse yet, the antivirus solution did not provide reporting or alerting, so by the time performance was impaired, the systems had to be manually cleaned and re-imaged. About every week, Elie would have to manually download a tool to several systems and remove malware. Each machine typically required 30 to 45 minutes to clean. If multiple workstations in a lab were infected, the lab was basically down until they could be cleaned up. In addition to taking valuable IT time, teachers lost the use of their systems during class, which resulted in having to change lesson plans on the fly.



And no one knew what malware was lurking on machines that were not covered by the antivirus software. Pop-ups, Potentially Unwanted Programs (PUPs), and other problems went unreported until the systems failed.

“Not only did we need better protection, we needed visibility into all of our systems,” said Elie. “And we needed a more efficient way to remediate malware and prevent it from gaining a foothold on our endpoints across the district.”

The solution

Malwarebytes Anti-Malware for Business and Management Console

After considering numerous options for fighting the malware epidemic, the school district selected Malwarebytes Anti-Malware for Business based on the recommendation of an experienced IT consultant. In his experience, Malwarebytes was the only anti-malware solution that enabled him to remediate systems that were previously unrecoverable.

Fast and convenient to deploy

Elie first had to manually remove the existing antivirus solution on the district’s machines. Once that was completed, Malwarebytes could be installed simultaneously to groups of systems from the Malwarebytes Management Console.

“Deploying Malwarebytes was so much faster and easier than anything we’ve deployed,” said Elie. “Updating systems will be a snap in the future. In addition, our district has limited connections to the Internet. Because Malwarebytes updates are small and we can schedule them for a convenient time, we don’t have to worry about bringing Internet access to a halt during the school day.”

Protection in real time

Malwarebytes will be installed on all of the district’s endpoints. For the first time, the district will be able to see the malware that threatens its systems and proactively address it before students or staff report machine performance problems.



The future looks bright

The Klamath-Trinity Joint Unified School District is moving toward a 1:1 computing model, and Malwarebytes will be a key component of its success. With more endpoints to manage, Elie says that he will save hours, if not days, of time with the ability to automatically scan endpoints, push out updates, address malware remotely—and do it all without disrupting instructors’ teaching or students’ learning processes.

“Malwarebytes gives us a tremendous comfort level,” said Elie. “We don’t have to constantly worry about threats. Now we have the tool we need to move forward to 1:1 computing with confidence.”

| 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