Malwarebytes

CASE STUDY

Enterprise Elementary School District expels malware

Malwarebytes Endpoint Security keeps staff PCs clean, digital curriculum flowing, and students learning

INDUSTRY
Education

BUSINESS CHALLENGE
Proactively prevent malware from infecting faculty and administrators' PCs

IT ENVIRONMENT
Primary data center with firewalls, iboss Cloud Secure Web Gateway, and Kaspersky antivirus

SOLUTION
Malwarebytes Endpoint Security, which includes Anti-Malware, Anti-Exploit, and the Management Console

RESULTS
- Reduced malware infections from 1,000 to almost zero
- Saved the IT team hours each week by eliminating the need to clean and re-image individual PCs
- Automated scanning and reporting for instant visibility into malware

Business profile

The Enterprise School District began in Redding, California, in 1884 with a small building and 15 students. Today it educates 3,700 students across nine schools and is actively incorporating digital curriculum into all grade levels. When malware threatened to hinder employee productivity and disrupt teaching, the IT team expelled malware as a threat to students' learning.

> We needed a tool that could proactively prevent, detect, and clean up malware. We found this in Malwarebytes.
>
> —Eric Zane, Technology Director, Enterprise Elementary School District

Business challenge

Proactively prevent malware

Approximately 250 teachers and administrators rely on Windows PCs to carry on the business of education. Recently, the district's IT team found itself increasingly bogged down cleaning and re-imaging PCs. A rising tide of malware was crippling PC performance, and the district's content filter had detected infected machines' attempts to communicate data to outside control system IP addresses. The lean IT staff spent approximately six hours each week cleaning or re-imaging machines.

"The more we cleaned, the more malware we found," said Eric Zane, Technology Director at Enterprise Elementary School District. "It was time to do something about it."

The solution

Malwarebytes Endpoint Security

Zane and his team began looking for a better way to deal with malware. They needed a solution that would add another layer of defense to their existing content filter and antivirus.

"We found a number of tools that could detect and quarantine malware, but not clean it up," said Zane. "We could use Malwarebytes individual installs to clean it up, but nothing was proactively preventing malware from getting in."

Using Malwarebytes Endpoint Security, the team conducted a pilot project on 100 machines. In the first week after deploying Malwarebytes, the software identified 1,000 instances of malware, including toolbars and Chrome extensions.

"That's when we realized how many malware problems we really had," said Zane, "and the only way to combat malware is to prevent it. We deployed Malwarebytes Endpoint Security on all of our employees' systems."

Malwarebytes Endpoint Security provides a powerful multi-layered defense engineered to defeat the latest, most dangerous malware, including ransomware. It includes Malwarebytes Anti-Malware, Anti-Exploit, and the Management Console in one comprehensive solution. Malwarebytes Anti-Malware detects and eliminates zero-hour malware, Trojans, worms, rootkits, adware, and spyware in real time. It stops threats in their tracks and saves Zane from having to manually remove malware from endpoints. Malwarebytes Anti-Exploit adds even more defenses against malware. Four layers of protection work together to block exploits and prevent malicious payloads from being delivered.

Rapid deployment and simplified management

The IT team used the Malwarebytes Management Console to install the Malwarebytes software on all of its machines. The console became invaluable for deleting and remediating threats that the software quarantines. The team set policy to automatically scan all systems each week and to check for Malwarebytes updates. Reporting capabilities keep staff apprised of endpoint status and identify threats.

"Frequent scans and the reporting capabilities let us jump right in and do whatever is needed," said James Boling, Scripting Specialist for Enterprise Elementary School District. "It's a huge help to keeping machines clean."

Effective and time-saving

Malwarebytes Endpoint Security provides a highly effective layer of security that complements the school's content filter, which sits on the edge of the network at the Internet connection. Now, malicious threats rarely survive long enough to infect users' PCs. Infections dropped from 1000 to an occasional browser redirect that requires removal.

"Our machines have been malware-free since we deployed Malwarebytes," said Zane. "It's a huge relief and a tremendous time-saver, since we're not spending hours every week cleaning infected machines."

End users have regained valuable time, since their PCs no longer have to be taken down for cleaning or re-imaging. Most importantly, they have full use of their machines with no malware-related performance impacts.

Next stop: servers

As the school district moves to incorporating digital curriculum, server-based applications and teachers' machines have become mission-critical. When the school district began using Malwarebytes Anti-Exploit, it quickly identified malware that was attacking Java applications on servers.

"We had one server that became severely infected with malware and we almost had to rebuild it," said Zane. "Malware was robbing the server's CPU resources and brought it to its knees. That could have had serious impact on our applications and on teachers' classroom activities."

Now, Zane and his team are deploying Malwarebytes on the district's Windows servers. Malwarebytes dramatically reduces risk to its servers.

"Our kids need the hope for their future that education provides," said Zane. "We're here to make sure that their progress is not disrupted by malware."

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