

Forsyth County Schools get an A+ in reducing risk with real-time protection

Malwarebytes delivers up-to-the-minute visibility

INDUSTRY

Education

BUSINESS CHALLENGE

Reduce risk associated with malware

IT ENVIRONMENT

Windows Defender antivirus, firewalls, content filtering

SOLUTION

Malwarebytes Endpoint Security

RESULTS

- Gained real-time visibility into potential threats
- Protected against zero-day threats
- Tailored policy to a range of different environments
- Reduced malware intervention from multiple times per day to less than once per week

Business profile

Forsyth County Schools (FCS) began in 1873 when several log buildings built in cleared fields were consolidated into one public district. Today, FCS serves more than 47,000 students and employs 5,000 staff members. The district is proactive when it comes to security protection. Starting in kindergarten, students are taught the importance of computer security, and staff is trained to recognize common cyberthreats. When FCS wanted to add another layer of security to its endpoints, it chose Malwarebytes.



Malwarebytes checked all the boxes, especially for zero-day infections. The more we read, the clearer it became that Malwarebytes caught new threats faster than other solutions.

—Tim Fleming, Director of Technology, Forsyth County Schools

Business challenge

Accelerating visibility into system status

FCS is home to 37 schools—21 elementary schools, 10 middle schools, 6 high schools, and one virtual 6-12th-grade school. In 2018, a new high school and the Alliance Academy for Innovation, a college and career high school, will open. The district boasts three national Blue Ribbon Schools and students with some of the highest ACT scores in the state.

Recently FCS upgraded its teachers' systems to notebook computers, enabling them to have greater access to Internet resources. At the same time, the IT team wanted to implement better protection for the new systems. FCS staff was frequently targeted by phishing attempts and Internet Explorer exploits.

“We needed more protection than just Microsoft Defender,” said Chad Abbs, Senior Network and Systems Administrator for FCS. “We also needed better reporting with real-time notification about threats, exploits, and blocked sites.”

In the past, threat reports were generated at the end of the day. The team wouldn't be able to read them until the next morning, so it could be 24 to 48 hours before they could investigate a machine and



remediate any infection. Real-time reporting would reduce dwell time and the risk of damage from threats.

“We had a list of requirements for a new solution,” said Abbs. “In addition to better protection and reporting, we wanted to make sure it didn’t affect endpoint performance or inconvenience users during scans. We wanted centralized management and the ability to easily set and change policies. We also needed a solution that automatically updated itself and could catch zero-day infections.”

The solution

Malwarebytes Endpoint Security

FCS tested a wide range of potential solutions, including Symantec, AVG, Malwarebytes, and others. Abbs and other team members also reviewed feedback on tech forums from other organizations and school districts.

“Malwarebytes checked all the boxes, especially for zero-day infections,” said Tim Fleming, Director of Technology for FCS. “The more we read, the clearer it became that Malwarebytes caught new threats faster than other solutions. We went ahead and purchased Malwarebytes Endpoint Security.”

The team created install packages tailored to each school, which simplified management, and rolled everything into the imaging system to deploy the new systems.

It works

Malwarebytes significantly reduced the number of systems needing investigation from multiple per day to fewer than one a week by blocking ransomware and other exploits. It constantly scans systems and delivers real-time alerts so the team can address potential issues immediately.

“Before, if a system was infected on Monday, we might not know until Friday,” said Abbs. “Now Malwarebytes detects threats in real time and alerts us, giving us an edge in reducing dwell time and lowering the risk of potential damage.”

Flexible management

FCS will be replacing systems in the school computer labs, which serve a variety of purposes—from supporting normal productivity software and online learning programs to enabling students to explore programming. Malwarebytes gives the team flexibility to protect all systems without generating false positive alerts for approved—but less common—software. For example, systems in engineering labs where students use Android development software will be protected without generating constant alerts.

“Malwarebytes is a standout enterprise solution,” said Fleming. “We can deploy different policies for each site and for unique environments, and we have the flexibility to accommodate everything from development labs to low-cost PCs that we want to lock down.”

Real-time reporting

“We love the email alerts,” said Abbs. “The time savings have been huge. We don’t have to constantly run reports just to know what’s going on. We can handle an incident immediately instead of having to spend an hour logging into the system to see what might be going wrong.”

Instead of 24 to 48 hours, now the team can respond in about 15 minutes to get a machine off the network if necessary. Abbs said that Malwarebytes reporting is easy to use and delivers reports instantly. In the past, running a report often took the management server offline because of the load.

Next steps

FCS continues to focus on cybersecurity education for students and staff in addition to progressively enhancing its security posture. Malwarebytes is already automatically installed on new systems, and it will be deployed district-wide in 2018.

“We also operate a large VSphere and VSAN environment supporting virtual servers and desktops,” said Abbs. “We plan to have Malwarebytes protecting those systems as well.”

| 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