

# Trussville City Schools



## Sanctuary Enables Innovative School System to Safely Incorporate Technology into the Learning Process without Being Hindered by Viruses, Spyware or Malicious Applications

### Background

In July 2005, Trussville City Schools ([www.trussvillecityschools.com](http://www.trussvillecityschools.com)) in Trussville, Ala. officially seceded from the Jefferson County School System and formed its own K-12 school district, comprised of five schools and 4,150 students. As part of this move, Trussville realized that information technology represented an untapped learning tool capable of helping its students and teachers improve the learning process.

Administrators developed a comprehensive technology program that included implementing the Microsoft Learning Gateway Framework. Using the Microsoft SharePoint portal server, Trussville enables students, teachers and administrators to securely access the district's network to post blogs, podcasts and other innovative learning tools. Trussville's technology plan also called for issuing a laptop to all teachers as well as all students in the sixth grade and higher. While this program is cutting-edge among school districts, it created various security challenges that needed to be addressed.

### The Challenge

According to the Children's Internet

Protection Act (CIPA), enacted by Congress in December 2000, schools must certify that they have an Internet safety policy and technology protection measures in place. An acceptable policy must include technology protection measures to block or filter access to offensive material and to monitor online activities of minors. Providing a laptop to every teacher and student created a need for additional security for Trussville to comply with CIPA requirements.

Shawn Nutting, director of technology at Trussville City Schools, found himself with a dilemma. "When it comes to student computing, Trussville takes a much different approach than the typical school district," said Nutting. "Schools are generally conservative, completely locking down student workstations or limiting access to certain programs and applications. In Trussville, the technology staff's primary goal is to prepare students for the future. We want both teachers and students to benefit from the tremendous advances in information technology. However, we have to consider CIPA requirements as well as our machines' health and the district's IT investment."

### The Solution and Benefits

To address his concerns, Nutting purchased SecureWave Sanctuary® Application Control. Sanctuary is an endpoint security solution that creates a whitelist of allowed applications while denying all others by default. This includes all viruses, spyware and other forms of malware, all unwanted programs and all unauthorized software. "Sanctuary helps us create a safe computing environment by giving the IT department control over what programs are allowed," said Nutting. "Instead of completely locking down

machines or prohibiting access to the Internet and other programs, we can work with teachers as they develop their digital curriculums. Approved software can quickly be added to the whitelist, ensuring that students are equipped with the technology needed to support a more complete learning experience."

In addition to its application control capabilities, Sanctuary's monitoring functionality enables Nutting and his staff to view those executables—including malware and unauthorized software—that were downloaded but failed to run because they were not on the whitelist of authorized programs. After deploying Sanctuary, Nutting was surprised to find out how many different applications were trying to run on Trussville's network.

"I was amazed—and certainly concerned—by the amount of spyware trying to execute on our machines. There were also several Trojans that got by our anti-virus software and had spread to numerous machines," said Nutting. "It turns out, about a dozen users—including students—had been running various U3 applications by connecting their USB memory sticks or other devices to our machines. We also found quite a few unknown applications that could easily have been malicious. Sanctuary simply blocked these executables because they were not on our allowed whitelist."

### Conclusion

Trussville City Schools has gained national attention because of its advanced and innovative technology program. Many wondered how the school district would be able to provide the amount of access it promised without jeopardizing

students' safety or Trussville's IT investment. Thanks to SecureWave's Sanctuary endpoint security software suite, Nutting and his staff were able to safely execute the district's technology plan.

"Many school districts preach the benefits of incorporating technology into the learning process, but they struggle with how to control access without inhibiting students," said Nutting. "Sanctuary enables Trussville to take advantage of new

technologies while preventing any viruses or unauthorized software from compromising the well-being of our students or the condition of our laptops and PCs."



**SecureWave**  
Safeguarding Tomorrow

[www.securewave.com](http://www.securewave.com)  
[info@securewave.com](mailto:info@securewave.com)

#### North America

13755 Sunrise Valley Drive  
Suite 203  
Herndon, VA 20171  
United States of America  
+1 (703) 713 - 3960 Phone  
+1 (703) 793 - 7007 Fax

#### United Kingdom

Midsummer Court  
314 Midsummer Boulevard  
Milton Keynes MK9 2UB  
United Kingdom  
+44 (0) 1908 357 897 Phone  
+44 (0) 1908 357 600 Fax

#### Continental Europe and Rest of World

Atrium Business Park  
23, rue du Puits Romain  
L-8070 Bertrange  
Luxembourg  
+352 265 364-11 Phone  
+352 265 364-12 Fax

© 2007 SecureWave SA. SecureWave and Sanctuary are registered trademarks of SecureWave SA.  
All third party trademarks are the property of their respective owners.

Trussville City Schools - Apr. 07 - V2.0