



## Faronics Layered Security and Augusta County Public Schools

April 19th, 2011

# Faronics Layered Security and Augusta County Public Schools

## Background

Augusta County is located 100 miles west of Richmond in the central part of the Shenandoah Valley of Virginia. Augusta County Public Schools (ACPS) has 21 schools including five high schools, four middle schools, and twelve elementary schools. There are approximately 1,750 staff and 11,000 students operating on over 4,000 workstations and over 80 servers.

## Problems

### Frequent System Downtime Due to Infections

For years, the district was struggling with accumulating support issues related to malware attacks on staff and student computers. On a daily basis, the technicians at Augusta County Public Schools were spending over 60% of their time fighting malware infections and repairing computers. On multiple occasions, it took several technicians from ACPS's busy IT department over a week to clean up a malware infection that plagued the district systems.

### Lack of IT Resources to Handle the Ever Increasing IT Requests

The constant battle of remediating machines prevented the technicians at ACPS from focusing on more important projects to propel the schools forward technologically. With over 4,000 machines to manage, the technicians needed a fast effective solution to help alleviate the burden of the rising IT support requests.

### Security and Compliance Challenges

Teachers and students often brought in malware infections by accidentally clicking on a malicious link or file. There were a few incidents where the Conficker worm (whose objective is to hijack computers completely, steal personal information, or commit basic extortion) demanded money for fake anti-virus software claiming to remove the infection.

Such malware attacks posed significant risks to the variety of confidential data that ACPS safeguards. From student records to medical and financial records, the importance of keeping the data safe was critical since ACPS has requirements to meet compliance mandates under both Family Education Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA).

“ Our systems are up and running without disruption and IT doesn't need to spend weeks to clean up infections. ”

## Solution

ACPS chose to implement a layered security strategy for their workstations and servers to ensure all their challenges were resolved. This layered security strategy involved three layers, all managed through one central console from security software provider Faronics.

Faronics Anti-Virus ensures that any known malware threats are contained, while Anti-Executable's application

whitelisting protection tackles all threats that evade anti-virus solutions, from zero-day attacks to spear-phishing and unwanted programs. Finally, Deep Freeze protects workstations by restoring computers to their original state with a simple reboot.

## Outcome

### Reduced IT Support Requests by Over 60%

The technicians first implemented Deep Freeze across their entire district six years ago, leading to a 60% reduction in daily IT requests. Deep Freeze helps eliminate workstation damage and downtime by making computer configurations indestructible. Once Deep Freeze is installed on a workstation or server, any changes made to the computer are automatically erased upon a simple restart.

### Increased System Availability

Although Deep Freeze is 100% effective at removing or recovering any new information written to a protected area with every restart, ACPS realized they still required additional security layers to protect computers during computer runtime.

The software needed to be able to deliver anti-virus updates without delays even on computers in Frozen mode (protected by Deep Freeze). Standard anti-virus solutions required workstations to be in Deep Freeze maintenance mode to deliver updates, which left computers vulnerable to malware infections since they weren't updated in time.

"Faronics Anti-Virus has been a godsend with low impact on system resources and a full integration with Deep Freeze to deliver updates without putting Deep Freeze in maintenance mode," said Amos Painter, IT Technician at ACPS. "It's performed better than other anti-virus solutions out there; an install-and-forget-about-it type of solution". Amos pointed out that deploying Faronics Anti-Virus made the life of the IT team easier since it was managed through the Faronics Core Console, a centralized management system for both Deep Freeze and Faronics Anti-Virus.

"Most of our computers now have Faronics Anti-Virus installed and it's helped us standardize our anti-virus environment a lot," said Amos. "Our systems are up and running without disruption and IT doesn't need to spend weeks cleaning up infections."

### Enhanced Security for Endpoints and Servers

The IT department attributes much of their security success to securing both endpoints and servers. The team has deployed Faronics Anti-Executable on over 75% of its servers to ensure that any threats that evade anti-virus are stopped before they infect servers and endpoints.

"Once we implemented Anti-Executable, it has become impossible for cyber attacks to infect our systems," shares Shaun Portlock, a Computer Technician with ACPS.

"Anti-Executable is very powerful on the servers, blocking zero-day attacks, targeted attacks, and programs we simply don't want in our environment. Since application whitelisting is not dependent on signatures like anti-virus, there's no risk that a new, unknown threat will evade it and therefore infect the network."

The Conficker worm attacks that previously plagued the district were successfully eliminated by Anti-Executable thereby minimizing IT time and resources required to remediate infected systems. "Anti-Executable on the server prevented the Conficker executables from running ensuring we have solid, stable servers and protected endpoints," recalls Shaun.

Anti-Executable works on a whitelisting principle, allowing IT to specify all the good programs permitted to execute on a server or an endpoint. The infinite number of bad applications and malware is simply ignored and never allowed to run. “Anti-Executable controls the servers and in the rare event that something may go through, we can simply shut down the server,” informs Shaun.

### Fulfill HIPAA and FERPA Compliance

ACPS stores financial, medical, and student records for its staff and students, which it is mandated to protect by compliance regulations such as FERPA and HIPAA.

“Faronics Anti-Virus, Anti-Executable and Deep Freeze help keep all our data safe and mitigate liabilities and risks of lawsuits from parents and students in the event that their data is lost or stolen,” said Amos. “When we submit our required documentation to the State and Federal government, we outline the three solutions as proactive ways we keep our staff and student data secure.”

Faronics Anti-Virus and Anti-Executable are particularly helpful in protecting data from exposure and loss to malicious third parties therefore helping ACPS comply with regulations and avoid embarrassing and costly security breaches.

With a complete layered security strategy in place, the district can now rest assured data is protected, computers are up and running without interruption, and staff and students can continue to do their jobs productively. Moreover, IT has reduced costs, decreased the number of IT requests, and become more proactive in handling critical projects instead of reactively fighting fires.

### About Faronics

With a well-established record of helping businesses manage, simplify, and secure their IT infrastructure, Faronics makes it possible to do more with less by maximizing the value of existing technology. Faronics is the ONLY endpoint security software vendor to offer a comprehensive layered security solution consisting of anti-virus, application whitelisting, and instant system restore protection. Incorporated in 1996, Faronics has offices in the USA, Canada and the UK, as well as a global network of channel partners. Our solutions are deployed in over 150 countries worldwide, and are helping more than 30,000 organizations.



[www.faronics.com](http://www.faronics.com)

Faronics helps organizations increase the productivity of existing IT investments and lower IT operating costs. Incorporated in 1996, Faronics has offices in the USA, Canada, and the UK, as well as a global network of channel partners. Our solutions are deployed in over 150 countries worldwide, and are helping more than 30,000 customers.

**CANADA & INTERNATIONAL**  
609 Granville Street, Suite 620  
Vancouver, BC  
V7Y 1G5 Canada

**Phone:** +1-604-637-3333  
**Fax:** +1-604-637-8188  
**Email:** [sales@faronics.com](mailto:sales@faronics.com)  
**Hours:** 7:00am to 5:00pm  
(Pacific Time)

**USA**  
411 Old Crow Canyon Road, Suite 170  
San Ramon, CA  
94583 USA

**Phone:** 800-943-6422  
**Fax:** 800-943-6488  
**Email:** [sales@faronics.com](mailto:sales@faronics.com)  
**Hours:** 7:00am to 5:00pm  
(Pacific Time)

**EUROPE**  
Siena Court, The Broadway  
Maidenhead, Berkshire,  
SL6 1NJ UK

**Phone:** +44-1628-509008  
**Fax:** +44-1628-509118  
**Email:** [eurosales@faronics.com](mailto:eurosales@faronics.com)  
**Hours:** 7:00am to 5:00pm

**COPYRIGHT:** This publication may not be downloaded, displayed, printed, or reproduced other than for non-commercial individual reference or private use within your/an organization. All copyright and other proprietary notices must be retained. No license to publish, communicate, modify, commercialize or alter this document is granted. For reproduction or use of this publication beyond this limited license, permission must be sought from the publisher.