



Faronics Anti-Executable and Granite School District

Case Study
February 26, 2009

Intelligent Solutions for **ABSOLUTE** Control

www.faronics.com

Tel: 1-800-943-6422 • Fax: 1-800-943-6488

Tel: +1-604-637-3333 • Fax: +1-604-637-8188

© 1999 – 2009 Faronics Corporation. All rights reserved. Faronics, Faronics Anti-Executable, Deep Freeze, Deep Freeze Mac, Deep Freeze Linux, Faronics Device Filter Mac, Faronics Insight, Faronics Power Save, Faronics Power Save Mac, Faronics System Profiler, and WINSelect are trademarks and/or registered trademarks of Faronics Corporation.

All other company and product names are trademarks of their respective owners.

Faronics Anti-Executable and Granite School District

About Granite School District

Granite School District, located in Salt Lake County, Utah, operates 60 elementary schools, 16 junior high schools, 9 high schools, as well as other special schools and programs. With 68,075 students, Granite is the second largest district in Utah and is among the largest public school districts in the nation. Granite is also one of Utah’s largest employers, with more than 7,500 full and part-time employees. Granite has also been nationally recognized for teacher professional development programs and the economic efficiencies of its administration.

The Problem They Faced

Scott Watson, an Electronics Teacher in Hunter Senior High School, trains students in a computer lab consisting of 24 workstations that operate as independent computers 90% of the time, and server-interfaced network stations for the balance 10%. These dual-core processor systems run Microsoft Windows XP SP3 and are utilized by over 150 students every day.

“We are fortunate in that we have a powerful computer lab,” says Mr. Watson. “We do, however, want to ensure that power is used for educational purposes, and not for classroom distractions such as games, instant messaging, and peer-to-peer file sharing.”

Mr. Watson continues, “We found that as the prices for USB flash drives fell, more students were using the drives to bring portable applications and executables into the classroom. This is obviously something we don’t want since the applications students need to complete class assignments are already installed on the computers. Allowing unauthorized programs to run on workstations presents a serious challenge to a teacher’s ability to keep lab computers running and student attention focused.”

“Allowing unauthorized programs to run on workstations presents a serious challenge to a teacher’s ability to keep lab computers running and student attention focused.”

The Solutions They Tried

The district did have a software product installed on the lab computers that kept unauthorized software from being installed on workstations; however it did not block program execution if the software was totally contained in the USB flash drive or any other source. As a result, the effectiveness of the current solution was reduced since it was not keeping up with technological and market changes.

Scott started looking for newer, better products that could block unauthorized and unwanted executables from running—regardless of where the executable is located. “We were already using Faronics Deep Freeze on our systems to keep them clean and consistent,” says Scott. “When I visited the Faronics website and discovered Faronics Anti-Executable, I knew it was something I had to try out.” Granite School District is using Faronics’ flagship system consistency product, Deep Freeze, to eliminate workstation damage and downtime. Once Deep Freeze is installed on a workstation, any changes made to the computer—regardless of whether they are accidental or malicious—are never permanent.

Now Scott was excited about Faronics Anti-Executable. Its ability to only allow approved applications to run on a computer is exactly what he needed. Any other programs—whether they are unwanted, unlicensed, or simply unnecessary—are blocked from ever executing.

The Solution That Worked

“I could not find any other product comparable to Faronics Anti-Executable,” says Mr. Watson. Faronics Anti-Executable has given Granite School District the ability to enforce total compliance in their computer labs. The district’s teachers benefit from distraction-free classroom sessions each and every time, while the district’s IT personnel are guaranteed that the lab computers remain free of unwanted software and compliant with acceptable use policies.

“Faronics Anti-Executable’s white list protection gives us the assurance that only the programs we have installed on the computers are able to run,” says Mr. Watson. “We use Deep Freeze to return our computers back to their original state, but that happens only upon workstation restart. Sometimes a lab computer is kept running for an entire day, so it could potentially accrue a whole day’s worth of ‘software junk.’”

“White list protection gives us the assurance that only the programs we have installed on the computers are able to run.”

What Mr. Watson is referring to, of course, are keyloggers, spyware, malware, viruses, and trojans. These unwanted pieces of software can seriously cripple computing sessions, create damaging privacy leaks, and hamper student productivity. Faronics Anti-Executable protects students from these threats while still allowing them to access the programs needed to complete class assignments. Faronics Anti-Executable also ensures that at any given time only fully-licensed software is running on the lab machines.

“As a test I asked my class of extremely tech-savvy students to have a go at trying to hack or cripple Faronics Anti-Executable,” says Scott. “After a week of unsuccessful attempts, the students have voted Faronics Anti-Executable to be bulletproof.”

Some of the ways in which the students tried to bypass Faronics Anti-Executable’s protection include:

- Replacing the administrator account
- Renaming unauthorized program names to authorized program names
- Program execution via batch files
- Replacing the white list file
- Hacking the computer management information



FARONICS
ANTI-EXECUTABLE

Key Benefits

Block Distractive Software From Running

- Blocks distractions such as games, instant messaging clients, and P2P applications from executing
- Ensures that computers are used for their intended purpose

Stop Malicious Software From Installing

- Protects users from software threats—such as keyloggers, spyware, & malware
- IT personnel experience a reduction in helpdesk requests

Keep Workstations Compliant

- Guarantees that computers are compliant with acceptable use policies, regulatory requirements, and software deployment schedules

Scott continues, “They were never able to bypass Faronics Anti-Executable. My favorite feature of Faronics Anti-Executable is its ability to read an authorized executable’s ‘fingerprint’ so that even if one tries to fool Faronics Anti-Executable with a renamed program file, it will not execute. Very smart, indeed.” ■



Faronics delivers software that helps manage, simplify, and secure desktop computers. Our products ensure users enjoy a trouble-free computing experience, and have freed IT personnel from tedious helpdesk requests. Faronics’ products benefit educational institutions, healthcare facilities, libraries, government organizations, and corporations in over fifty countries worldwide.

Contact Us

Web: www.faronics.com
Email: sales@faronics.com
Phone: 800-943-6422 or 604-637-3333
Fax: 800-943-6488 or 604-637-8188
Hours: 7:00am to 5:00pm (Pacific Time)
Address: 170 – 2411 Old Crow Canyon Road 620 – 609 Granville Street
San Ramon, CA 94583 USA Vancouver, BC V7Y 1G5 Canada

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, and thereafter it may not be re-copied, reproduced, or otherwise distributed. 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.