

Aspire to a Network Free of Malicious Programs

Since 1947, Aspire of Western New York has served children and adults with cerebral palsy, intellectual disabilities, epilepsy, autism and other neurological impairments, striving to let them live as independently as possible. To that end, Aspire's five main offices, 42 group homes with 24-hour care, one school and a medical clinic serve as many as 3,000 patients and residents throughout the region.

Aspire's computer network ties all of these locations together, providing Web and email access to roughly 400 administrators, medical and finance staff, residents and students. With an IT staff of just three to cover this sophisticated and geographically diverse network, Aspire can't afford to allow malware, spam and viruses to regularly disable PCs and servers. The organization now uses Webroot in the cloud and on the desktop to filter traffic, protect PCs from viruses, malware and other malicious programs, and easily enforce remote use policies.



The Problem

In February 2009, the malicious virus "Sality," which spreads rapidly through infected .exe and .scr files, as well as via a Trojan that can bring additional malware into the network from the Web, attacked Aspire. The security software from Trend Micro was ineffective at stopping this virus, and within days, 40 PCs both inside and out of the corporate firewall, and five servers across the organization's main offices were rendered inoperable.

"Our finance department was dead in the water for four or five days," says Dave Compton, Aspire's system administrator. One terminal server, providing Web access to the 42 group homes was also infected, knocking out its online capabilities. His team and another consulting firm rebuilt each machine, costing enormous amounts of time and money.

Why Aspire of Western New York chose Webroot:

- Malware and virus detection and blocking
- Web filtering
- Remote access control
- No on-site server
- Cost Savings
- Superior support

Additionally, without Webroot, residents and students had unfettered Web access, often logging on to the type of sites that host the most malicious viruses and malware. Each week, two or three group homes were infected with the latest bugs, knocking out multiple PCs and requiring a member of the three-person IT staff to drive as far as two hours each way to fix the infected machines.

"The product [we were using] wasn't seeing or catching anything, and I just can't afford to have people traveling that far, simply to return a week later for another virus," says Compton. "It became laughable."

The Solution

Compton knew he must find a powerful replacement, and watched Webroot's online demonstration a week before his old security software license was set to expire. With that, he signed on to test Webroot on seven machines. "Webroot was more than helpful in giving me all the tools needed to demo the solution," says Compton.

Within the week, Aspire activated Webroot® Web Security Service and Webroot AntiSpyware Corporate Edition to protect 400 users from malware, viruses and other malicious programs, and also installed Webroot Email Security on over 700 email accounts. In fact, at that point, Compton was still curious whether Webroot would catch the spyware and malware that had previously avoided detection. "But all of a sudden, it got quiet at the houses," he says.

Desktops were no longer becoming infected or disabled because Webroot Web Security was blocking the incoming malware—even on the residence computers that are not behind the Aspire firewall.

The IT staff now isn't spending its time on the road. And as Aspire rolls out Webroot's desktop software across the residences, Compton creates user groups of those PCs to enforce acceptable use policies and filter Web traffic accordingly. He's able to control all of this from his office via the Webroot management portal, and because Webroot is a SaaS offering, Aspire didn't require additional hardware to implement the solution.

"Only by doing this in the cloud am I able to extend the reach and control of my security," says Compton. "I can do everything from here. That's huge."

Comments

"Only by doing this in the cloud am I able to extend the reach and control of my security. I can do everything from here. That's huge."

**—Dave Compton
System Administrator
Aspire of Western New York**

Webroot Software, Inc. – USA
2560 55th Street
Boulder CO 80301 USA
www.webroot.com • 866.915.3208

Webroot International Ltd. – EUROPE
Alexandria House, The Sweepstakes, Ballsbridge
Dublin 4, Ireland
www.webroot.com/europe

Webroot Software Pty Ltd. – APAC
Level 20, Tower A, 821 Pacific Highway
Chatswood NSW 2067 Australia
www.webroot.com/au • +61 (0)2 8448 8144 • 1800 029 234

© 2010 All rights reserved. Webroot Software, Inc. Webroot, the Webroot icon, Spy Sweeper and the Webroot tagline are trademarks or registered trademarks of Webroot Software, Inc. in the United States and other countries. All other trademarks are properties of their respective owners. NO WARRANTY. Analysis based on research conducted by Webroot Software, Inc. The information is provided AS-IS and Webroot makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at your own risk. Documentation may include technical or other inaccuracies or typographical errors. Webroot reserves the right to make changes without prior notice. Certain data is available upon request.