webroot

Case Study

Richmond Ambulance Authority

Richmond Ambulance Authority Turns to Webroot® to Protect Mobile Devices

Richmond Ambulance Authority (RAA) provides Emergency Medical Services (EMS) to more than 200,000 people across Richmond, Va., making it one of the busiest per-capita systems in the nation. The EMS industry has shifted in recent years from solely providing patient transportation to also using mobile technology that improves patient care. RAA has proactively integrated innovative systems within its vehicles and was named a finalist for Computerworld's "Best Practices in Mobile & Wireless" Award. At RAA, strategically deploying cutting-edge technology not only improves operational effectiveness – it helps to save lives.

The Situation

On January 1, 2009, RAA deployed a wireless computer system throughout its fleet of 40 ambulances. Laptops and docking stations were installed in each vehicle so emergency medical technicians could access and disseminate patient information from the field. With the ability for information like EKGs and other vital stats to be sent directly to doctors, patient care was greatly improved. Now, RAA paramedics can quickly and efficiently communicate information for the 100-plus patients they transport each day.

The tablets (CF-19 Panasonic Toughbooks) were using a mobile gateway to obtain Internet access, with encryption software to ensure that private information remained secure as it passed between servers. Antivirus software from another vendor was installed to prevent malware. However, the existing solutions failed to address Web filtering and Internet policy enforcement, which were vital issues given RAA's line of work. In an emergency situation every second can be crucial, and controlling Web surfing in the field would help to ensure the fastest possible paramedic response times. RAA needed a comprehensive Web security solution that would allow administrators to monitor and manage Internet activity while providing an extra layer of protection against Web-based viruses, spyware and other complex threats.

The Solution

Jerald West, Senior Mobile IT Specialist at RAA, also works as a part-time computer technician at Best Buy and was a strong proponent of Webroot's consumer security products. He had used Webroot System Analyzer to run scans for potential threats on customers' computers and found it to be highly effective. "I knew Webroot had the technology to do a lot of the things we were looking for in terms of blocking spyware and viruses," West explains, "so I started looking for a business solution that could protect computers not tied to the network.

Comments

"Webroot Web Security SaaS was the perfect solution for our mobile users. We can protect the computers not tied to our internal network and control Web activity in the field. Webroot helps us to ensure the integrity of our organization – and it also saves us money by preventing any harmful viruses and spyware from infecting our mobile computers. Our CTO is so impressed by the benefits that we are considering implementing the solution on our desktop computers as well.

I chose Webroot because of their outstanding reputation and they have not let me down. The customer service is outstanding. We look forward to continuing to work with Webroot for many years to come!"

– Jerald West
Senior Mobile IT Specialist,
Richmond Ambulance Authority

Webroot Web Security SaaS was ideal. All you have to do is use a proxy address and point it to the Webroot data center, and all the Web traffic is routed through there."

Webroot Web Security SaaS (Software-as-a-Service) prevents Web-based threats by scanning all HTTP and FTP over HTTP requests in the cloud. Because the Webroot service sits at the Internet layer, laptop users can authenticate directly with the service rather than establishing a VPN connection back to the server. Webroot provides a Service Level Agreement (SLA) to guarantee 99.99 percent uptime and defense against 100 percent of known viruses and spyware. A zero-hour heuristic filter protects against new and unknown threat variants, and advanced heuristics identify phishing sites in real-time in order to help keep sensitive data secure.

The Benefits

Alleviating Web traffic to the server not only simplifies Web access for users, but it also eases management requirements for RAA. In addition, RAA finds that Webroot's policy enforcement and reporting capabilities are extremely beneficial. The IT team is able to monitor and manage Internet activity though a centralized administration console, which also provides access to real-time user logs, charts and data.

To help control Web browsing, Webroot groups millions of URLs into 12 main categories and 96 subcategories. This enables RAA to block categories not related to medical needs – such as adult content or social networking – while permitting access to useful categories such as education and government. Customized "allow and deny" lists enable administrators to add individual Web sites that could be beneficial for paramedics to access. Detailed reports display which sites and downloads users have attempted to access, so RAA can gauge individual user activity and gain insight into overall traffic trends and blocked viruses.

With Webroot Web Security SaaS in place, IT administrators can rest assured that Web surfing and Internet threats will not endanger patient care, while RAA paramedics have access to the life-saving technology and information they need.

Webroot Software, Inc. – World Headquarters
2560 55th Street
Boulder CO 80301 USA
www.webroot.com • 800.870.8102

Webroot Ltd. – EMEA Headquarters
Cart Lodge, Squerryes, Goodley Stock Road
Westerham, Kent TN16 1SL, UK
www.webroot.com/uk • +44 (0)870 1417 070

Webroot Software Pty Ltd. – APAC Headquarters
Level 20, Tower A, 821 Pacific Highway
Chatswood NSW 2067 Australia
www.webroot.com • +61 (0)2 8448 8144 • 1.800.029.234

USA-240309-1.3