

Reliable Virus Protection Keeps Your Systems' Guard Up

Software diseases are more contagious than ever – and clinical networks and medical systems are certainly not immune to them. But a new Virus Protection solution via Siemens Remote Service (SRS) can deliver protection to help keep your medical systems healthy.

By Eric Johnson

Life, Siemens' unique customer care solution, is dedicated to helping customers get the most out of their investment from the moment of purchase. The latest service aimed at achieving this goal is Siemens Virus Protection, a solution powered by Siemens Remote Service (SRS), the efficient and comprehensive infrastructure for a wide range of medical-equipment-related remote services. How critical is the need for such a service solution?

Since the mid-1990s, total healthcare expenditure in developed countries has grown at nearly 5 percent per year, double the rate of the overall economy. It now accounts for 5 to 15 percent of all spending and investment. However, there is a parallel healthcare boom – this one not for humans, but rather for computers. The disease responsible for this boom is malicious software, or "malware":

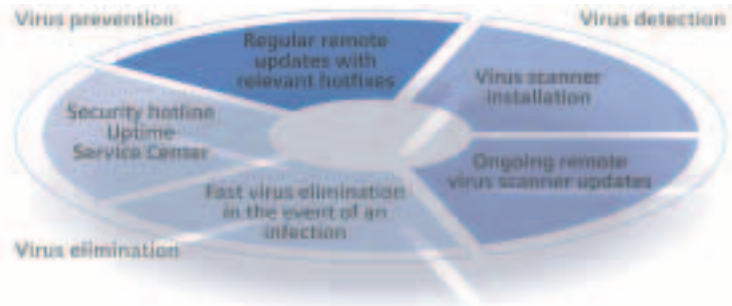
viruses, worms, trojans, time bombs and denial-of-service agents.

Now for the Bad News

The damage can be massive, running into the billions of dollars. And monetary consequences are just the beginning: lost data and wasted time are also a major problem. A recent virus, "Sircam", for instance, went so far as to forward the contents of infected machines. Just imagine, last month's expense account plus your entire personal calendar sent out for inspection by friends and neighbors, not to mention customers and competitors.

In the medical sector, malware's potential harm is even greater. Faulty software could delay or even foil diagnoses and treatments. A "Sircam"-style spreading of medical data would grossly violate patient privacy.

Siemens Virus Protection – From Start to Finish



As if all this weren't bad enough, another unfortunate truth is that even more crises can be created if a computer infection is fought too hastily. An untested "hotfix" from a software vendor could interfere with an imaging system's main functions. An unapproved virus scanner may dispose of or falsify genuine image data. Either of these may violate medical equipment standards, such as Europe's CE Mark or North America's UL Certification.

Siemens' White Knight Rides the Internet

The good news is that Siemens Virus Protection – protection ranging from virus detection to elimination and proactive prevention – can help you avoid being part of the aforementioned scenario. Developed and tested over the past year in Germany and the U.S.A., the service comprises three main components. The first is a carefully tested virus scanner from Trend Micro™, that continuously inspects all incoming and existing files on the system for infection. This works in the background, so as not to slow down the imaging system's primary function, and it is automatically remotely updated on a regular basis via a secure Internet connection.

If a virus is somehow able to get by the virus scanner and infect the system, it will run into the second component, a reliable virus elimination process. This alerts you, the user, without delay as well as the Siemens Uptime Service Center that a virus is present. Uptime Service staff then assist you in killing the virus and getting your system up and running again as quickly as possible.

The third component is a virus prevention tool. When Microsoft® sends out its hotfixes (update packages of files meant to solve a vulnerability in the operating system), Siemens inspects them to see if they are security-relevant for their syngo-based systems. If so, Siemens comprehensively tests the hotfix. Once validated, the hotfix is quickly transferred to your system via remote technology. Thereby, Siemens efficiently works to protect the system from the intrusion of new viruses. The key benefits for your facility? Outstanding

VIRUS SCANNER INSTALLATION

Siemens installs Trend Micro™ OfficeScan™, which continuously monitors your system for malicious attacks – without interrupting your clinical applications.

ONGOING REMOTE VIRUS SCANNER UPDATES

Siemens and Trend Micro routinely keep abreast of the latest virus developments. Automatic remote updates of the latest validated virus patterns and scan engine are installed during the system boot phase, so as not to interrupt clinical routine.

FAST VIRUS ELIMINATION

If a virus does get through to your imaging system, OfficeScan™ detects it and sends an alert to the Siemens Uptime Service Center (USC) without delay. The USC provides reliable support in eliminating the virus, restoring and recovering of your system – thus getting it back online again as fast as possible.

SECURITY HOTLINE

Siemens Uptime Service Center is available 24/7, 365 days a year as your immediate point of contact for up-to-date virus information, IT-security matters, as well as rapid response support regarding virus protection.

REGULAR REMOTE UPDATE WITH RELEVANT HOTFIXES

Proactive monitoring, careful assessment and validation on a product-specific basis of hotfixes released by Microsoft® to quickly provide your system with all IT-security-relevant updates from our remote location.

defense against malicious attacks, increased patient safety, system availability and therefore revenue, smoother clinical operations, rapid problem resolution, better staff planning through reduced security effort, and increased budget optimization. This all-inclusive protection will spare you from having to worry about the health of your imaging systems and allow you to instead keep your focus where it belongs – on the health of your patients.

Author: Eric Johnson, based in Zurich, writes about technology, science and business.