



130 Maple Avenue, Suite 7B
Red Bank, NJ 07701

Securing a PC Workstation: A Healthcare Technology Perspective

Version 2.0: August 25, 2005

Case Study: Healthcare Technology Provider

Company profile

THIS COMPANY HAS DESIGNED AN INTEGRATED PC WORKSTATION SYSTEM THAT UTILIZES A BREAK-THROUGH IMAGING TECHNOLOGY THAT ENABLES EARLY DETECTION OF AN EYE DISORDER. THIS EARLY DETECTION CAPABILITY FACILITATES BETTER TREATMENT AND IMPROVES THE EYE EXAM PROCEDURE THROUGH IN-OFFICE CONVENIENCE. IT IS QUICK AND EASILY ADMINISTERED BY A PHYSICIAN'S EXISTING OFFICE STAFF WITH MINIMAL TRAINING. DIGITAL IMAGES ARE AUTOMATICALLY TRANSMITTED OVER THE INTERNET FOR INTERPRETATION BY SPECIALISTS. IMPROVED MEDICAL TREATMENT ASSESSMENT, FASTER MEDICAL REFERRALS AND EFFICIENT INSURANCE CLAIM PROCESSING ARE THE ULTIMATE BENEFITS OF THE TECHNOLOGY.

Business situation

The leveraged technology was developed at a Mid-Atlantic USA research university that pursued the use of digital image technology to examine certain physical attribute of the human eye. The need for an improved technology to help detect a specific Eye Disorder was essential to provide an optimal healthcare technology for eye clinics, with installations in the 1000s, each a single location. The company successfully leveraged the new use of digital imagery to develop the first production version of an integrated PC Workstation for image capture and processing. This provided for the company's early insight into technology improvements and field support requirements for eye clinics utilizing the new system. The turnkey technology has been completely integrated and automated with the use of a PC running the Microsoft Windows Operating System.

Technical situation

This Healthcare technology provider required very specific improvements to an upgraded version of their solution. The company recognized a vital need for system performance improvements along with comprehensive needs for system security. The system processed detailed images of the retina that are needed to provide accurate diagnostic services for patients along with important and confidential patient information. A reliable and uncompromised image and information processing system has been and will continue to be essential.

Goals

The following performance and security improvements were needed to improve the future expanded field support requirements for all of the production, PC workstation systems:

- *Internet connections needed to be secured (for both industry patient confidentiality and for practical business reasons)*
- *PC users, not conducted patient services, needed to be blocked*
- *System resolution and camera speed needed to be upgraded*
- *Physical Field Support Requirements needed to be decreased/minimized*
- *Improvements for digital photo transmission times via dial-up VPN connections needed to be achieved*

Technical Requirements

The company implemented a hardened version of their integrated PC workstation solution and utilized Privacyware's Privatefirewall product to provide important security that solved two specific problems:

- *Unauthorized system use: Since the integrated solution was designed to only provide the diagnostic service for patients, all other attempts to use the computer needed to be blocked.*
- *Secure digital patient information transmissions via the Internet: The integrated solution connects and transmits data via the public Internet, utilizing a VPN. It was imperative that desktop security be rock solid and that security policy can only be set by an authorized administrator of the system.*

Privatefirewall™



and

Integrated PC Workstation with Image Capture and Processing Technology for Eye Clinics



The healthcare company contracted Privacyware to create a unique and customized configuration of Privatefirewall that accomplished the two goals above in the following way:

Unauthorized System Use: Privacyware established a solution that provided for “stealth” system security. The custom configuration of Privatefirewall provided for the blocking of any other attempted application load, other than the allowed applications needed to perform the patient service diagnostic procedure. Privatefirewall’s security software architecture enabled for the complete satisfaction of this important system security and system use policy. The attempted breach by a user would be prevented and a notification regarding this action would not be made available to the unauthorized user.

Secure transmission of digital patient information: At the time of dial-up connection, the company determined that its field systems were being scanned by hackers on the Internet, even though a secure VPN connection was being used. The system scans were attempting to access information about system IP addresses and potential installed services on the systems that could be exploited. An additional security policy had to be established utilizing Privatefirewall, that would block any system calls, or attempted connections, other than the specific patient information session that needed to be completed over the Internet. This included both attempted inbound unauthorized actions and any outbound unauthorized actions.

Benefits

The company completed its existing field unit upgrades and they have started a complete rollout of new systems to eye clinics. The use of the Windows based operating system provided for an easy integration of the image capture and processing application. But this same use of MS-Windows created system performance concerns that they were able to address with Privacyware's Privatefirewall™ product.

Specifically, the company's new field production units were upgraded with faster processors and are running Windows XP Professional. The company knew they needed more than just the existing Microsoft security measures in Windows XP.

There are basically two categories of threats that can compromise a personal computer, even an integrated, turnkey and "hardened" personal computer, such as this healthcare company solution. These threats fall into either an inbound and outbound category. Defined as:

Inbound – these are system security threats that come from outside the system or the computer network, wherever an Internet and/or network connection exists on a computer. These threats include port scans, executable software, Trojans and viruses that can be installed by accessing a malicious Website without warning. Some of these types of threats are both inbound and outbound in nature where an inbound threat actually creates an outbound threat.

Outbound – these are system security threats that originate on local systems. These include malware, downloaded software, outbound packets containing personal information from installed software and keyloggers. Some of these types of threats are both inbound and outbound in nature where an inbound threat actually creates an outbound threat.

Industry statistics suggest that the current survival time of an unprotected system on the Internet is only 16 minutes. Certainly, this company realized right away that the hacker scans, when a patient information transmission session was established, were threats on their systems.

First, the company knew that the Windows XP's built-in firewall was not enough. This solution did not protect them from outbound threats. **Many PC users still do not realize that the Windows Firewall only protects from inbound threats and not outbound.**

Second, they knew that the Windows Firewall could not be customized with a specific stealth policy, such as the one created with Privatefirewall that optimized a security solution that improved field system reliability by providing specific and direct security on the installed computers.

"Working with Privacyware on our system security requirements has been and continues to be very professional. Privacyware's ability to scope our security needs was impressive. They enabled us to continue to improve our technology and field support requirements, without compromising system performance due to our security needs."

-CIO of this Healthcare Technology Provider

Results

The completed system upgrades and new system deployments now have improved overall productivity.

- *System processing and session transmissions times have improved by nearly 100%*
- *Non-standard field support calls have decreased substantially through the improved field security*
- *System reliability has improved with the use of Windows XP Professional operating system and Privatefirewall.*
- *Image resolution and camera image processing capacity increased with simple hardware upgrades that were easily managed through Windows XP Professional and security with Privatefirewall.*
- *Field system deployments have increased by nearly 500%, with an increasing number of systems to reach nearly 1000 within the coming year. This could not have been achieved without improved performance and security.*
- *Essential security compliance requirements have been implemented which is a key requirement for HIPAA regulations.*

The complete integrated PC workstation solution specifications are as follows:

- *Personal Computer with MS-Windows XP Professional Service Pack 2*
- *Specialized Digital Camera with magnification with Filter: Red free (green filter)*
- *Light: 100w halogen lamp*
- *Dimensions: 24" length, 18" width, 21" depth*
- *Weight: 55 lbs.*
- *Angle: 55 degrees of diagonal coverage*
- *Power Supply: Computer 230w, Motor 50w, Lamp 150w*
- *Power Consumption: 100-125 VAC; 50-60 Hz*
- *Modem (Internet Feed): Dedicated analog phone line for direct dial-up connections*
- *Stand: Provided with locking wheels with electronic height adjustment*
- *Integrated image capture and processing application*
- *Touch Screen technology with application navigation made simple*
- *Instructions: Set-up, testing, troubleshooting and interactive operator training information is provided (digitally embedded) in the application*
- *Privatefirewall v4 (custom build) for application specific functions, with user and Internet security protection policies*
- *Patient Chair: chair with arms, no wheels*

Privacyware™ and Privatefirewall™ are trademarks of PWI, Inc. Products and trademarks from other companies mentioned herein are for identification purposes only and may be registered trademarks of their respective companies. Specification is subject to change without notice.

2005© PWI, Inc. dba Privayware™. All rights reserved.