Case Study

Portwell, Inc.

ST. JOSEPH HEALTH SYSTEM

Building a Trusted Network
Portwell's CAR-3000

1U Rackmount Communication Appliance for Network Security

Portwell

St. Joseph

Serving the Brazos Valley since 1936

Situation

St. Joseph Health System is an integrated local healthcare system with facilities in the seven-county primary service area of the Brazos Valley, Texas. The majority of its health services are delivered at St. Joseph's main campus, the regional health center based out of Bryan, TX. This facility provides a range of inpatient, outpatient and surgical specialties and shares vital patient information with associated physicians' and doctors' offices, as well as critical access hospitals located in Brazos Valley. As St. Joseph Health System Network Specialist, Alan Williams is responsible for the secure, timely and accurate sharing of this vital patient information between his headquarters in Bryan and the county locations.

Williams' networking group needed to run voice, data and some video down the communications tunnels set up between Bryan and its "remote sites" and ensure the patient information exchanged with these clients was secured and encrypted to comply with HIPAA guidelines and policies for privacy of patient information.

Looking to Extend the Network

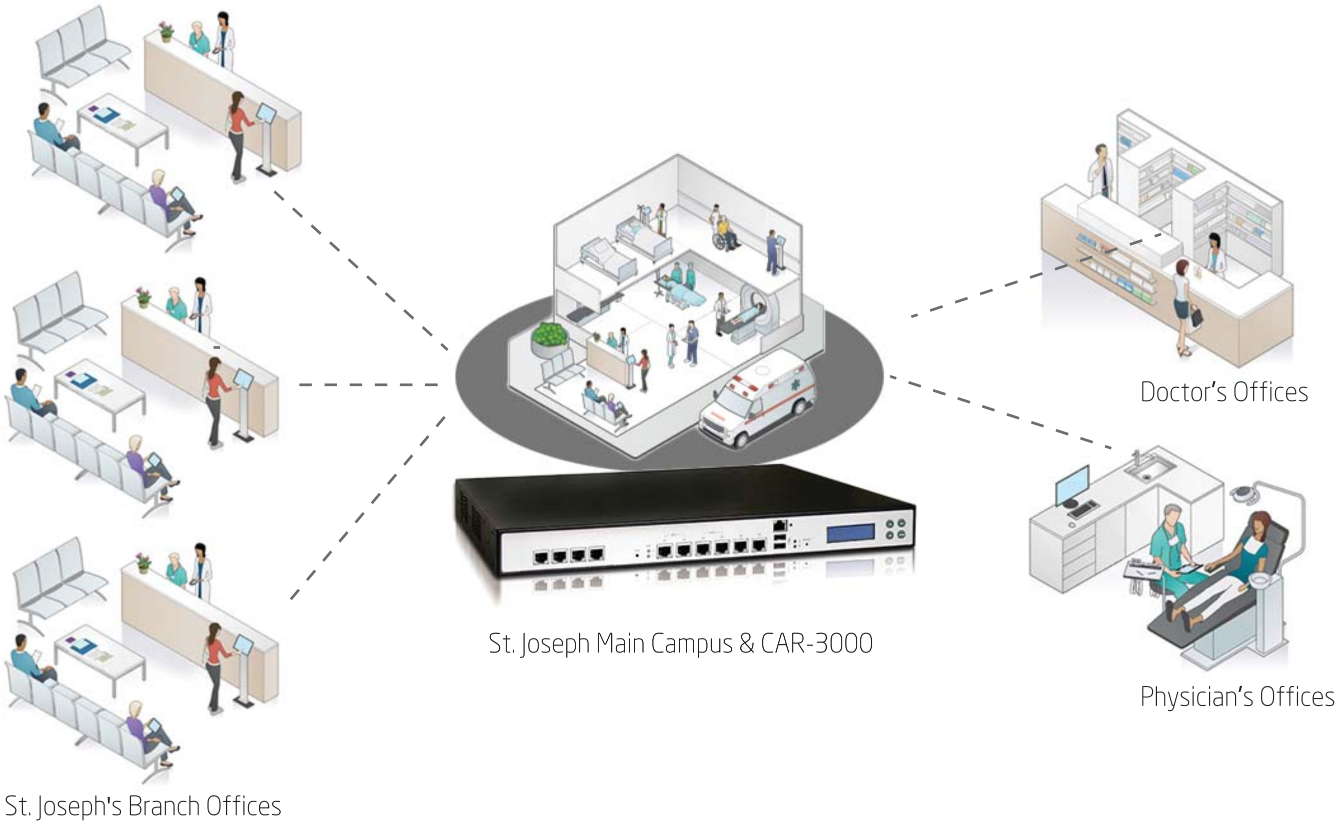
"These connections were untrusted networks, so we had to encrypt the data that flowed between Bryan and the branch offices," Williams explains. "Before we contacted American Portwell Technology, we were using Layer 3 encryption devices. We had implemented a system from another supplier that provided an all-in-one solution through a box that already had the encryption function folded in. All I had to do was just configure it."

The problem was, this original solution did not meet Alan Williams' needs. "It wasn't robust enough for us," Williams notes. "It was probably fine for home use. But this was a new situation for us and we had obviously underestimated our needs," he confesses. "As we built our connections, we realized there was no way this system would handle the amount of traffic we were pushing through it, so we went back into the market to find a more powerful, more robust and more elegant solution.

"In addition, Layer 3 hindered us," Williams says. "It wouldn't allow us to extend our network and that's exactly what we were looking to do because we wanted to provide more services. So we needed greater flexibility than the original solution could provide."

intel

Intelligent Systems Alliance Premier


Doctor’s Offices
Physician’s Offices
St. Joseph Main Campus & CAR-3000
St. Joseph's Branch Offices

Finding the Software Solution

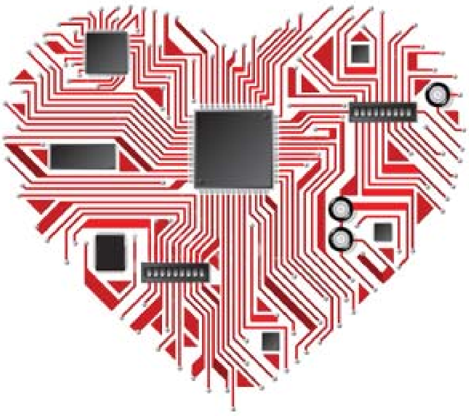
According to Williams—who instigated the project and took responsibility for its eventual success—he knew he did not want another PC-based solution. So he split the project into two segments: the encryption software and the hardware that would support it. Williams, a longtime advocate of Open Source systems, felt confident he could solve the encryption software side himself and soon found a suitable solution in an Open Source package using Linux and Open Source VPN solution.

“The encryption ‘box’ takes the packet data, encapsulates it in the encryption protocol and then distributes and supports it,” Williams explains. “The other side strips it off so the hospital and the remote network don’t even know there’s something between them, since the packet is not altered in any way.”

Seeking the Hardware Solution

At that point, Williams began his search for the hardware: a more transparent encryption device that would enable his team at Bryan to send any kind of encrypted packet across the network. "In addition to knowing what I did not want, I had a very clear idea of what I did want," Williams states. "We have a multiple-server that we call our encryption device at headquarters that feeds the several tunnels to the remote sites. So I knew I wanted a device that had multiple network ports and Gigabit connections. It also needed to be compact. We're limited for space," Williams explains, "so if we have six tunnels, we can't necessarily have six devices, which meant we had to maximize the Ethernet ports density on a single device. It was in our search for such a device that we discovered American Portwell Technology."

Williams began his search for the perfect device by inputting keywords such as "network security appliance" and "1U security appliance" into the Google search engine, then began a systematic appraisal of the results. Finally, he focused on CAR-1000 and made an online request for further information to American Portwell. This began a dialogue between Williams and Ellis Liu, American Portwell's inside sales representative. As the conversation progressed, Mark Huang, American Portwell's product marketing manager became involved. It was at this point that Liu and Huang suggested Williams consider CAR-3000, a much more sophisticated and scalable device they felt would better suit his needs and enable Williams to move to his goal of Layer 2 switching, which makes the transport virtually invisible.



Finding the Perfect Solution

"We recommended CAR-3000 because it is a compact and modular 1U rackmount communication appliance that is purposely built to address network security needs like St. Joseph's," Huang states. "It was designed and built with industrial grade components with a higher Mean-Time-Before-Failure (MTBF) for mission-critical applications." Huang confirms that CAR-3000 is also more scalable than CAR-1000 because it supports wide range of Intel® LGA CPUs from entry-level Celeron® 440 through Core™ 2 Quad Q9400 and everything in between. It also supports the latest dual-channel DDR3 1333/1066 memory platform up to 8GB and contains multiple Ethernet ports to protect different network segments. "Its compact 1U form factor is the perfect space and energy saving solution to Alan Williams' drive to provide flexible network security while cutting costs," Ellis Liu adds.

"As far as we were concerned, CAR-3000 worked pretty much out of the box," Williams says. "American Portwell simply added CPU, memory and a CF card with a VGA cable. There were no extra modifications and that was one of the many things that drew me to American Portwell in general and CAR-3000 in particular."

Williams had several criteria when he began his search for a 1U network appliance: The first was cosmetics. He definitely did not want another PC sitting on a rack. "I wanted something that looked elegant," Williams states. "I was also attracted by the fact that CAR-3000 features Intel Gigabit ports and Intel processors. No disrespect to other manufacturers, but I feel much more comfortable with a device that's Intel-based," he confirms. "Intel has an excellent track record within the Open Source community, which gives me confidence and peace of mind."

Solving the Problem

Satisfied with what he had seen and heard, Alan Williams ordered his first two units in April 2011 and put them through a rigorous load- and latency-testing program. Six months later, the project went live and by April 2012, Williams had ordered a total of nine units, with another seven due to ship before end of year. "Every time we get a connection to a remote site and can utilize CAR-3000, we do," Williams confirms. "As far as I can see, as we keep growing, we'll keep deploying the devices . . . and the project is expanding dynamically. What's more, it worked well from day one and has been working fine ever since. Any problems or questions I may have—and they have been few—are always handled quickly and professionally by Ellis and Mark."

"This is a mission-critical application for many of our access hospitals," Williams continues, "and has to operate 24/7 using our Hospital Information System to exchange vital patient information and records between remote sites and headquarters. Obviously, the solution has worked well for me and I would definitely recommend it to my peers in other healthcare systems and hospitals."

CAR-3000

American Portwell Technology's CAR-3000 is a compact and modular 1U rackmount communication appliance that is based on Intel G41 Express chipset. It offers a wide range of support from Intel Core 2 Quad Q9400 through Core 2 Duo E7400 to Pentium® E5300 and Celeron 440 and everything in between. It also supports: the latest dual-channel DDR3 1333/1066 memory platform up to 8 GB; one 3.5˝ or two 2.5˝ SATA HDD or SSD; up to six GbE RJ45 onboard ports with two software controlled bypass segments (Fail-Open or Fail-Close); expansion capabilities include one PCI-E x8 interface for a modular bay for Portwell's NIP module product family; fiber and copper port connections including dual-port 10G readiness (Intel 82598EB and Intel 92599ES with SFP+ Interface), LCD display module options that include EZIO-300 (2 x 16 character with 4 buttons), EZIO-G400 (128 x 32 graphical module with 4 buttons) or EZIO-G500 (128 x 64 graphical module with 7 buttons); and VGA pin-header available for software/application development.

About American Portwell Technology

intel
Intelligent Systems Alliance Premier

American Portwell Technology (http://www.portwell.com) is a wholly owned subsidiary of Portwell, Inc., a world-leading innovator in the industry of Communication/Network Security Appliances and a Premier member of the Intel Intelligent Systems Alliance. American Portwell designs, manufactures and markets a complete range of communications appliances, embedded computer boards and systems and rackmount systems for both OEMs and ODMs. American Portwell is an ISO 9001:2008, ISO 13485:2003 and ISO 14001:2004 certified company.

For More Information

www.portwell.com