



The Citadel

Citadel Implements PatchLink Update™ to Support Network Productivity & Security

A Tradition of Excellence

The Citadel — Military College of South Carolina is best known for its high academic standards and strict military discipline. Established in 1842, Citadel cadets have experienced many famous military engagements firsthand, from the Spanish-American War in 1898 through to today's battles in the Middle East. The Citadel exemplifies both "bravery" and "resilience."

Today, the picturesque campus, which comprises 24 buildings, offers a sophisticated technology infrastructure that meets both professor and student requirements. There is an enrollment of approximately 1,900 cadets and 19 degree programs are offered. Women were admitted into the Corps of Cadets in 1996. Moreover, U.S. News & World Report ranked The Citadel among the best colleges in the region in their reporting of "America's Best Colleges."

Manual Patching: A Hard Fought Battle

The Citadel realized it was in need of automated patch management when the SQL Slammer and Nachia viruses came on the scene in 2003.

The Citadel's Network Support Services Manager George Russ explains, "Both viruses brought various parts of the college's network to a halt. In addition, other viruses like Gaobot and its variants, while not as widespread, affected a number of students and faculty PCs, which further caused a major loss of productivity. Manual patching was our first attempt to relieve the virus pain."

“ When Slammer hit, we had to manually repair and patch almost two thousand student PCs. ”

Robert Palmer - Network Administrator

The Citadel's Lead PatchLink Administrator Robert Palmer continues, "We initially took the 'patch-all at once, sneaker-net' approach. When Slammer hit, we had to manually repair and patch almost 2,000 student PCs. After this, we added a Microsoft SUS Server but it only patched Windows 2000/XP PCs and did not cover the multitude of other non-Microsoft operating system vulnerabilities that exist."

After experiencing firsthand the maladies of manual patching, Russ and his team decided to search for a more comprehensive and automated solution to patch management, leading him to evaluate PatchLink Update™. A rigorous research and testing process left PatchLink Update standing alone as the only patch and vulnerability management solution offering comprehensive detection and deployment capabilities that went far beyond the other vendor offerings.



KEY FACTS:

- Campus spanning 24 buildings with over 1900 students
- Cross-platform and multi-vendor solutions such as Windows, Novell, Linux, and Apple
- SQL Slammer, Nachia, Gaobot and other attacks compromised thousands of machines
- Manual patching and Microsoft SUS failed to provide an adequate solution



The Cross-platform, Multi-vendor Challenge

The Citadel's computing environment consists of Windows, Novell, Linux and Apple platforms. Given this state of "cross-platform, multi-vendor" affairs, Russ knew his team needed an automated patch and vulnerability management solution that was on par with the school's standard for excellence.

"Microsoft, Shavlik, and BigFix cater to a strict Windows Active Directory Domain environment," Palmer explains. "These solutions did not work for us because they only support Microsoft vulnerability patching and are designed to work from a top-down approach where the server initiates everything through Administrative Credentials. This server scenario just isn't the reality in a homogenous, non-Active Directory environment."

The Citadel Network Support Services team's environment does not include Active Directory (AD) or administrative access to students' PCs. In this environment, IT cannot predict what firewall or other security software tool may be restricting communications and they have limited or no control to computers, such as laptops, accessing the college's network.

With these unknown variables in mind, Russ explains, "We are very concerned about the patch management process. Unpatched computers can be exploited in seconds causing loss of productivity, loss of data, and a reduction in network efficiency — all with the ability to negatively affect the mission of The Citadel."

“ Unpatched computers can be exploited in seconds; causing loss of productivity, loss of data, and a reduction in network efficiency. ”

George Russ - Network Support Services Manager

Increased Satisfaction & Reduced Costs

With PatchLink Update now in active operation for almost two years, The Citadel network support team is branching out and experimenting with other time and savings components offered by PatchLink, such as PatchLink Developers Kit™. Russ notes, "We are going to start using this tool because for the first time, we can now design custom detection and deployment packages that will meet our organization's in-house patch management requirements."

Moreover, PatchLink Update's mandatory baseline support assists Russ and his team in making sure all appropriate computers are patched and stay patched. "It is great to know that once we deploy patches using PatchLink Update, the computers remain patched even if a user decides to remove a patch or reloads Windows."

While precise total cost of ownership data is still being gathered, Palmer attests that the return on investment with PatchLink Update is immediate: "Our students and faculty experience fewer interruptions and the system administrators now make fewer computer maintenance trips to individual computers. These labor hours saved using PatchLink Update are priceless, not to mention greater satisfaction all around."

The Citadel's Network Support Services team today meets the college's high standard for excellence and itself can claim a higher degree of "resilience."