



# Case Study

BY JOHN WAGLEY

## Safely Connecting Computing Devices

How a network access control solution is helping a university safely connect new kinds of computing devices and operating systems.

**MANY ORGANIZATIONS**, especially larger ones, need to register and authenticate a growing number of computing devices onto their network. Some are looking for network access control (NAC) solutions that can quickly identify and authenticate new devices while also giving administrators flexible security and other controls.

One university, Colorado State, has found such benefits from SafeConnect, a solution from vendor Impulse Point. SafeConnect lets the university register and authenticate any computer that will access its network. In addition, it has the ability to quarantine at-risk devices when necessary, says university network security administrator William Davis. Since installing the solution, malware infections have dramatically declined, and the university has also been able to improve compliance with digital copyright laws, says Davis.

The university looked at several solutions when it began the search for a new NAC product a few years ago. One reason it chose SafeConnect was that, compared to some other solutions, it appeared to offer a broad range of security controls without excessively hindering users' Internet access, Davis says. It was especially important to find a solution that didn't have too many "false-positives" when it came to blocking access, he adds.

The solution was easy to install. With assistance from Impulse technicians, it took just a few days to connect to the university's existing network architecture, Davis says.

When students first try to log onto the network, they're directed to a SafeConnect Web page. They're then asked to cre-

ate a password, and an Impulse agent is downloaded to their device. This registration process helps ensure that people accessing the network are affiliated with the university. The SafeConnect agent helps the university set and control security and other policies.

Administrators can set policies based on factors such as whether devices have up-to-date antivirus or antispyware software or whether they're set to automatically download software updates and patches. Administrators can choose to block access to certain devices based on such criteria or to send messages warning users about those issues and helping them comply with existing policies.

Colorado State requires students to automatically update operating systems. Students who aren't set to receive automatic updates are provided with instructions and links to help them turn the function on.

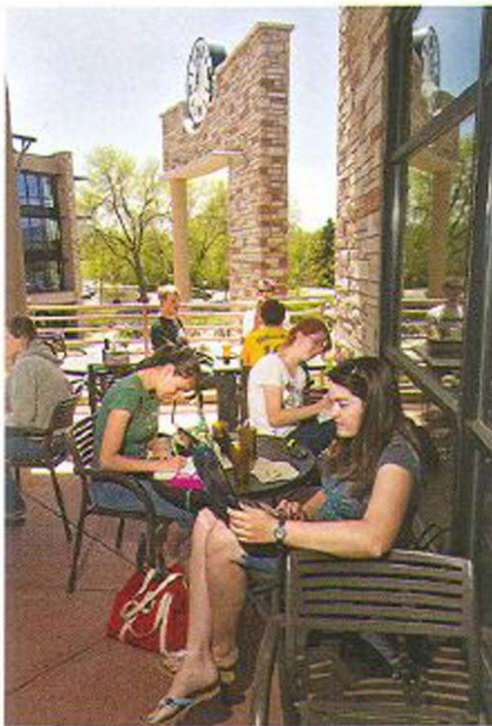
In the future, Davis says, the university may use SafeConnect's messaging function to communicate with networked students in cases such as security incidents. Messages could contain instructions telling students how to proceed, he says.

SafeConnect's automatic update policy has significantly cut cases of malware infection among student computers. Before SafeConnect, the university would receive about three to four calls daily, usually

about malware-infected devices. Since implementing the NAC solution, such calls have declined to just one or two a month, Davis notes. The university also hasn't had any widespread infections since installing the product.

Another major benefit of the solution is that it helps the university comply with digital copyright laws, says Davis. Increasingly in recent years, Colorado State and many other organizations have received takedown notices under the Digital Millennium Copyright Act. Such letters typically tell the university that copyrighted material appears to be freely available from a certain IP address, often through peer-to-

**COLORADO STATE UNIVERSITY** students can now safely connect their computing devices to the school's network.



## Case Study



October 2011

peer (P2P) file-sharing software.

Using SafeConnect's Web-based control module, administrators follow up on such notices by sending messages to the devices in question, says Davis. The messages "may say something like, 'in case you weren't aware, your system may be illegally sharing copyrighted material.'"

In many cases, students aren't aware that their songs are freely available to other Internet users, he says. Students are typically asked to remove their file-sharing software or the copyrighted material from their system. In some cases, the particular file-sharing program is mentioned in the takedown notice and relayed to the student.

If the university receives a third notice concerning the same student, that student's access to the network is blocked. This measure has only been used a few times, says Davis.

SafeConnect also offers a module that lets administrators block a host of known illegal P2P programs; the module can also direct users to legal sharing alternatives.

Impulse Point's customer service has been exceptional, Davis says. Though the university files trouble tickets relatively rarely, Impulse professionals are quick to respond and are almost always able to solve the problem, he says.

The price for SafeConnect starts at \$15,000 for 250 devices, according to Impulse Point. The price includes installation and training as well as a year of maintenance and support. Discount pricing is available for larger orders.

One possible, though minor, weakness of the solution, says Davis, is that it has been less effective at managing Linux operating systems compared to many others. But Davis says no more than about one percent of Colorado State's students use Linux.

Colorado State wanted a way to quickly register and authenticate a large—and proliferating—number of operating systems without hindering users' access. SafeConnect has helped the university accomplish this while bolstering security in a variety of ways, says Davis. ■

*(For more information: Anne Torgler, marketing manager, Impulse Point; phone: 863/904-6957; e-mail: [atorgler@impulse.com](mailto:atorgler@impulse.com).)*