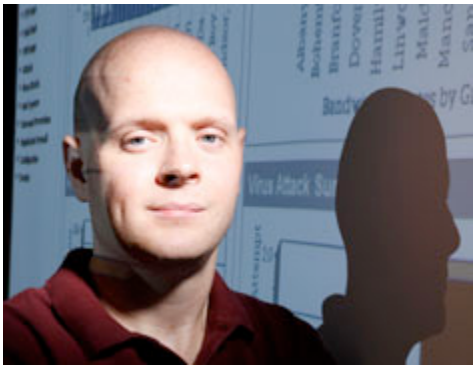
Case Study

Layered Security Lockdown

Premier Education Group adopts a defense-in-depth strategy to protect its most valued assets.

Karen D. Schwartz



Paul Somogyi protects Premier Education Group's campuses with network security gateways from SonicWALL.

Mark Battrell

With 10,000 students at 27 campuses through the northeastern United States, Premier Education Group's IT department has had its share of security issues. Over the years, it has seen just about everything, from students trying to surf inappropriate sites or download music from the Internet, to workstations without updated antispyware software and, worse, machines where the antispyware function had been turned off.

These issues have led to an array of problems, including unproductive students and staff, and slow-as-molasses connections. "If 50 people are listening to music online at one time, it will kill your bandwidth," notes Paul Somogyi, director of MIS for Premier Education Group, a privately owned career training organization based in East Haven, Conn.

By early 2009, it became clear that the school's approach to security was outdated and ineffective. The group decided to overhaul its approach to security by attacking it not only at the workstation level, but at the network and application levels as well.

"We needed security at every layer so we could make sure that nothing inappropriate was happening inside the firewall, and that nothing inappropriate could get in from outside the firewall," Somogyi

says.

Premier Education's move to a multilayered security approach is something every organization, regardless of sector or size, must do today to be secure. "With multilayered security, threats that circumvent controls at one layer can still be stopped by security set up for another layer," says Mark Bouchard, principal consultant at AimPoint Group of Millersville, Md.

UTM Migration

Somogyi's team chose a SonicWALL unified threat management appliance as its base security solution because it could tackle both the network and application security layers. Once it was delivered, the group took four months to get it up and running.

It installed one SonicWALL NSA 3500 UTM appliance in the network room at 24 of the campuses, and SonicWALL TZ Series appliances at a few of the smaller campuses. In some cases, the new units replaced older SonicWALL Pro 3060 security gateways, but many schools had no security gateway at all before the new appliances were installed.

The new UTM appliances serve as the Internet gateway and segment the campus network between staff and students. They provide a firewall, gateway antivirus and antispyware, intrusion prevention, content inspection, and the ability to evaluate Internet traffic based on its value to Premier Education through policies set up by the institution.

The benefits to installing the network security gateways were immediate. The intrusion prevention feature, for example, allows the IT department to block not only viruses, but also activities that aren't acceptable to the school's educational mission, such as online gaming, instant messaging and social networking. In addition, it allows the IT staff to scan for viruses at the gateway level, so even if a workstation is missing antivirus protection or the protection is out of date, the problem will be caught.

Central management is another benefit. With the addition of the SonicWALL Global Management System, which was installed on the SonicWALL E-Class Universal Management Appliance EM5000, the IT group can centrally manage and rapidly deploy

SonicWALL appliances and security policy configurations. The IT staff can also manage the appliances at all campuses concurrently and make global changes to blockor monitor a site.

"It takes a lot of trial and error to get network usage shaped the way we want it," says Ashley Torvinen, Premier Education Group's computer and network support technician. "The central management console allows us to make these changes quickly and efficiently."

For more on network security check out our E-Newsletter.

Reporting is another major asset of the Global Management System. "It allows us to see who is using the most bandwidth at certain times during the day," Torvinen explains. "If the network is very slow, for example, we can identify the computer using the most bandwidth at that time. We can even see what websites are being visited the most, and which machines are trying to access sites that we have

blocked.

“All of this information helps us fine-tune the network and increase bandwidth, something that had been a major problem before,” she adds.

In one case, the IT team had been notified from its Internet Service Provider that someone had downloaded copyrighted data from one of its campuses. With these tools, the team was able to quickly identify which computer the downloading had originated from and block the peer-to-peer software being used. With that information, the group was then able to make the proper changes at all campuses to prevent the problem from recurring.

Complete Protection

Once the SonicWALL equipment was in place and working well, the group tackled the endpoints and servers, turning to antivirus software and server protection.

For workstation security, IT deployed Grisoft’s AVG Anti-Virus scanning engine, which prevents users from visiting unsafe websites, as well as offering phishing and firewall protection, regular updates and remote management.

“We all know that antivirus software is only effective as long as it’s kept up to date, and that had been a problem,” says Ray Warner, a computer support specialist at Premier Education Group. “With the large number of PCs we have across the organization, the console makes it easy to keep track and update any PCs that have missed the auto-update virus definitions.”

For server protection, Premier Education Group installed Trend Micro ServerProtect, which provides real-time antivirus, antispyware and rootkit protection that is manageable by a single console. If ServerProtect finds a problem, it immediately cleans and repairs all servers where the problem has been located.

Now that the institution’s multilayer security strategy is complete, the next step is to create a testing lab to be even more proactive.

“We want to set up a testing lab and review and fine-tune the settings for the gateway and workstation protection so all future threats are prevented before we implement a new system in our production environment,” Somogyi says.