

Six things you should know about network endpoint security

Bert Latamore

July 06, 2006 (Computerworld)

"We as IT technicians are going about network security the wrong way," says Peter Green, director of IT at [Neumont University](#) in South Jordan, Utah.

"We are trying to put a box around our networks, when every night, a large portion of those networks leave the building, and in my case, [during every college vacation], those pieces scatter across 42 states.

You can't put a box around that. Neumont's environment is an extreme example for several reasons:

- The university offers only one undergraduate major -- a bachelor of science degree in computer science -- so its staff and student body are technically very sophisticated and can "circumvent any controls or security we can put in place and install whatever they want," Green says.
- Everybody carries laptops -- Lenovo ThinkPads. "We are completely mobile and wireless," Green says. "During the day, we have a huge network infrastructure, and at night, three-quarters of that network walks out the door."
- Because of the focus on mobility and wireless connectivity, the college has 80 Aruba A-band access points on two floors, connecting 400 laptops to 35 servers, four of them Senforce Technologies Inc. endpoint security and intelligent network access control (INAC) servers, over two networks. "A band works well particularly for classrooms because we can crank the power down to zero and pack a lot of access points into a small area," Green says.
- Students and instructors spend large amounts of time away from campus and take their ThinkPads with them. "If an instructor spends three months in Ireland, who knows what happens to his laptop?"
- The university has a constant stream of visitors, many of them from companies in its enterprise partnership program, which gives students experience working on real projects with professionals. These visitors bring their own laptops on campus and need connectivity to their companies and to the students in their workgroups.
- The university, however, has the same concerns as any other large organization. It wants a standard image across all of its laptops to facilitate maintenance, and "we are dealing with highly sensitive information on our network -- grades, projects for enterprise partners, personal information about students and staff," Green says.

"Our endpoint security discussion started when we got an excited call from our Cisco rep about an acquisition," Green says. "As a result, we had a conversation with Cisco about network access controls that fascinated me. To me, this is the future of the network. It made me realize that we have been looking at security from the wrong perspective."

But, he says, "when we asked about different features, the answer was always, 'We are working on that.' So when Senforce approached us with a fully based solution, we didn't look much further. This is so new that there isn't much out there, and Senforce has endpoint security and INAC together, which is great."

However, as with any new technological approach, endpoint security has its trade-offs, both in terms of money and changes in how IT approaches issues.

Green says that users should consider the following before committing to an endpoint security system:

1. This approach requires a more intelligent network, which usually means investment in extra hardware and software beyond the security package itself. "Many companies would have a lot of question marks. For us, the network is the center of our architecture, so we knew it was the right way for us to go," says Green.
2. "It fundamentally changes how you think about security," he says. "You are thinking less about internal routing and firewalling and more about individuals and clients, nodes and endpoints."
3. Visitor isolation is absolutely necessary and a big benefit of endpoint security. "Before we installed Senforce, wall-mounted plugs scared me. I didn't want a visitor coming in, plugging into the network, and accessing everything," Green says. "With INAC, who cares? If we cannot identify the user, then all we provide is a pipe to the Internet and the ability to initialize a VPN to their company. We find that this is the first thing visitors want in any case, and by the time our industry partners are ready to work with students, they are registered, and the network has ensured that they meet our standards for virus control and security."
4. A major danger of bleeding-edge technologies is that two years later, they can strand you with a proprietary system from a small vendor that lacks the resources to continue development, and ultimately require an expensive forklift upgrade to whatever standard has evolved. "One thing we like about Senforce is that its technology is already installed at DARPA, the Department of Defense and other leading-edge organizations," Green says. "That makes me feel pretty comfortable with this technology."
5. Leading-edge technology can challenge the IT staff's ability to adapt and can require extra time and effort. "We spent a year on this, but we believe the investment is worthwhile for our highly mobile environment," Green says.
6. Endpoint security requires active user involvement, at least to the point of responding when a pop-up comes on the screen informing the user that his laptop is quarantined until he upgrades his virus definitions or turns on his laptop's personal firewall. "We need to be sure our end users have that same emotional investment in the security of the network that we do. If they don't, they will see meeting security requirements as one more problem keeping them from their data," Green says. So user education is important. "We do get calls from people asking what these pop-ups are all about," he says. Explaining what seems obvious to annoyed users sometimes takes patience, so the help desk needs to be ready for those calls. "We also get calls from users who say, 'This is great. I can see exactly what I need to update to keep my system secure,'" Green says.

Overall, Green says, "We are in an enviable position in that we have the best people in the industry working for us, who know encryption and network access. This approach just makes sense for us."