

## **SpyForce-AI protects against insider threats**

### **Software uses artificial intelligence to detect anomalous behavior on networked systems**

*By Earl Greer, November 6 2006*

Information technology security managers are growing increasingly concerned about insider threats, which occur when employees compromise sensitive information stored on networked systems. With that in mind, we decided to test Nowell's SpyForce-AI, which uses artificial intelligence to monitor network use, to see if it could give us peace of mind.

SpyForce uses agents on each networked workstation, and the AI resides on a Red Hat Linux server. After setting up a Linux server, we grabbed a CD from the SpyForce product box and installed Cyclone server database software by following instructions from the printed manual. We also installed Nowell's Jenius server — pronounced "genius" — which handles the AI. We ran into some minor trouble with those installations because the instructions were for a different version of Red Hat than the one we were using. Under the circumstances, we would have liked Nowell to bundle a version of Linux with the product.

Nevertheless, we correctly set up the Nowell server software within half an hour. The manual recommends that you use one server for each domain, but you can disregard that if you are sure that each of your user names is unique.

Next, we manually installed the agent on each of our Microsoft Windows XP workstations. In each case, the Jenius server noticed our presence and began an interview with the workstation user. It presented questions in a teletypewriter format, which is old-fashioned but

effective. It asked each user different questions, but overall, we were satisfied that it gathered enough information to correctly identify each person.

We were happy to see that the interviews had a friendly tone that would encourage user cooperation. The interview took only a few minutes — not long enough to get tiresome — and the system accepted a range of input. For example, when it asks for your name, you can write "Jane Doe" or "My name is Jane Doe." And if you don't or can't answer a question, you can tell it to skip that question. The AI is not perfect. For example, when we said that we were in the midst of a drought in Texas, it said, "That's great." But if AI becomes perfect, there will be no need for us humans. The last installation step was to place the SpyForce-AI Security Tool, which is the product's management program, on a single Windows workstation. The Security Tool can manage the services on any SpyForce Linux server that you can ping, but each installation is set up to manage only one server.

### **Using SpyForce**

The AI needs some time to learn users' habits. Being impatient, we used the Security Tool to cut the required time from 40 hours of use to 10. After letting the AI get to know us for a couple of days, we decided to execute a file-compression program we had not used during the modeling time. SpyForce immediately said, "Hello," and politely asked if we would answer a few questions to be sure an evil twin wasn't trying to take control of the computer.

We were concerned at first that we would not remember the answers we had given to each question during the initial interview. Was our favorite sport knitting or skydiving? But the AI was smart enough to correctly identify us despite some wrong answers. We tried the same experiment again, this time deliberately giving all wrong answers. SpyForce gave us a polite message and then shut down

the computer, which is a more secure solution than freezing the display. The Security Tool quickly unlocked the workstation.

### What we like

At first, we thought the requirement for a Red Hat Linux server would be onerous, but we created the server with little cost or effort. Red Hat expertise would certainly be helpful, but someone with minimal experience should have no significant problems installing the server. We also liked the Security Tool. It allowed us to change the modeling time and tweak many other parameters, including SpyForce's sensitivity in detecting unusual behavior. It also let us choose the behavior changes that it would monitor, although you will probably want to accept the default settings.

In future versions of the Security Tool, we would welcome usage reports, such as a list of programs that each user executes. And it would be nice if SpyForce displayed at the top of the graphical user interface the name or IP address of the Linux server that the tool is monitoring.

### What we don't like

The management software provides detailed technical reports that are useful to administrators who are tracking specific events. But we could not find any reports that we could give to management executives to defend spending money on AI. However, you can import the text file into Business Objects' Crystal Reports or into your spreadsheet program to generate your own reports.

Because SpyForce does not have a deployment tool, installing it on all workstations in a large organization could be difficult, even using scripts. Large organizations might want to consider deploying SpyForce in selected departments that require heightened security.

### The bottom line

SpyForce-AI doesn't replace other security products, and it won't protect computers that don't connect to the network. But its

AI successfully catches most anomalous behavior. SpyForce-AI adds significant protection against insider threats, and it aids in complying with security regulations.

*Greer is a network security consultant. He can be reached at [egreer@thecourageequation.com](mailto:egreer@thecourageequation.com).*

### SpyForce-AI

#### Nowell, Inc

(512) 469-9779

<http://www.nowellgroup.com>

**Features:** \*\*\*\* (4/4 Stars)

**Performance:** \*\*\*\* (4/4 Stars)

**Usability:** \*\*\* (3/4 Stars)

**Platform support:** \*\*\*\* (4/4 Stars)

**Price:** \*\*\* (3/4 Stars)

**Price:** SpyForce-AI costs \$199 per computer.

**Pros:** The software can watch for unusual activity on networked workstations and quiz users to verify their identities.

**Cons:** The product does not have an automated means of deploying workstation agents, it lacks built-in management reports, and it requires a Linux server for each network.

**Platforms:** SpyForce-AI supports Red Hat Linux server and Microsoft Windows, Linux and Unix clients.

#### Counterespionage software

SpyForce-AI helps information security managers:

- Detect and help prevent employees from stealing or misusing information assets.
- Prevent intruders from using stolen identities, such as passwords and smart cards.
- Identify suspicious users and anomalous activity inside the network.
- Address internal security breaches in real time.
- Enforce new internal security regulations, such as those mandated by the Federal Information Security Management Act.
- Protect application servers, Web servers and databases from unauthorized use or access.

*Source: Nowell*