AKRON BEACON JOURNAL
Business

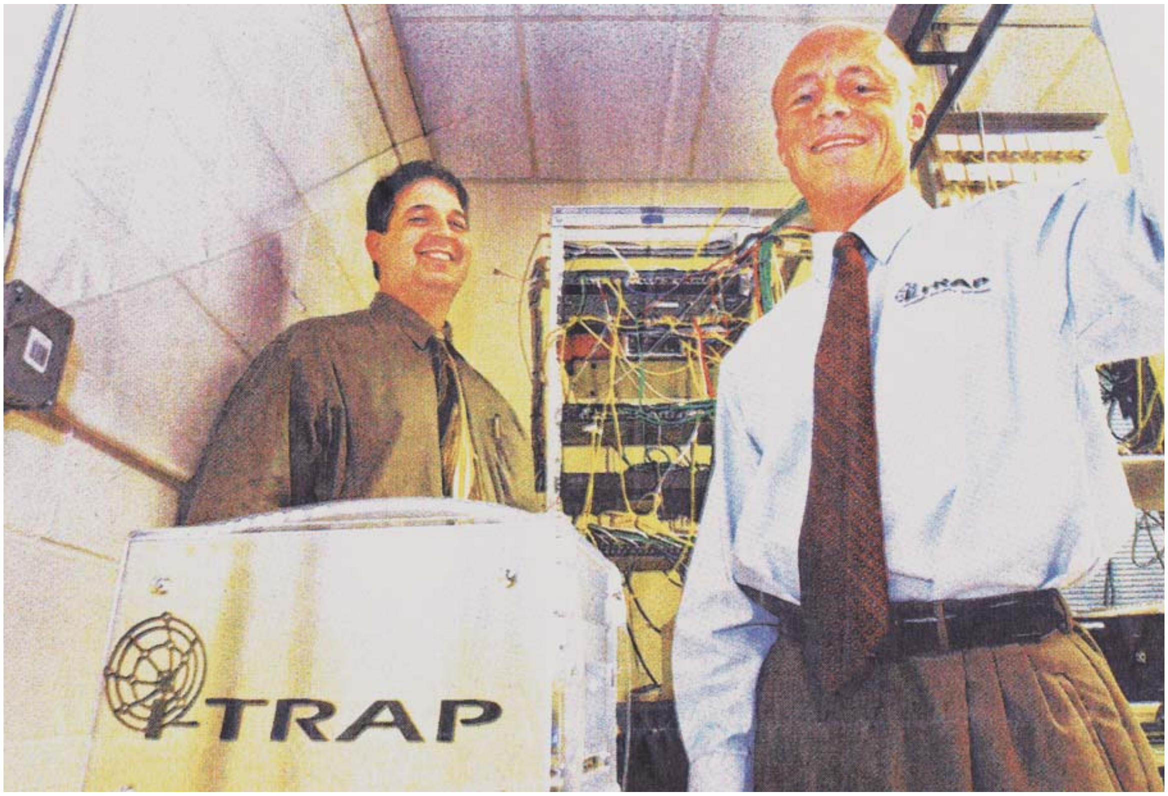
A song and a straw
Mini CDs on drink lids latest marketing gimmick.
D5

SEC. D
The Beacon Journal
Tuesday
July 1, 2003
www.ohio.com/business

Posted on Tue, Jul. 01, 2003

Local company keeps an eye on e-traffic

High security at low cost



Alex Desberg, marketing director, and John Clarke, general manager, showcase Bright.net's new security product, i-Trap.

Bright.net's i-Trap monitors firewall

By Erika D. Smith
Beacon Journal staff writer

Many people wouldn't think a sleepy town like Doylestown could offer much in the way of technology.

Silicon Valley it is not.

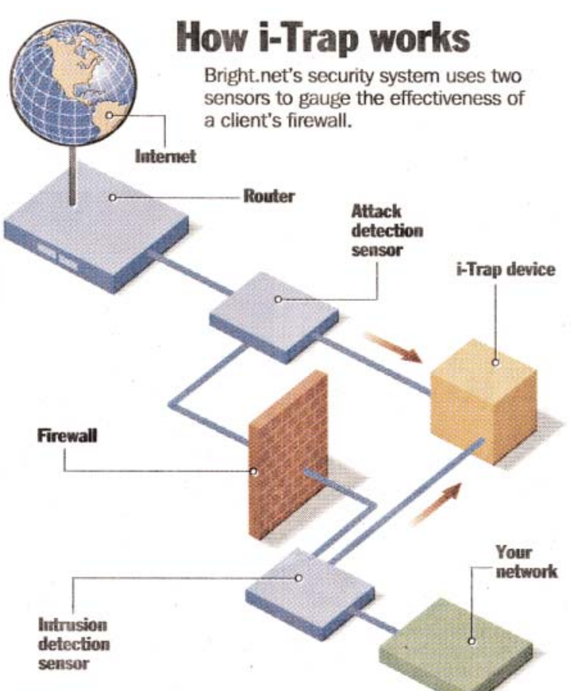
But tucked away in a few brick buildings in a corner of downtown, Bright.net is ready to break out nationwide with its new network security service.

I-Trap could be Bright.net's ticket into the burgeoning market of corporate computer security. Fifteen businesses in Ohio, including Barberton Citizens Hospital, already use i-Trap, and calls are coming in steadily from potential clients across the nation, said Marketing Director Alex Desberg.

The attention has come rather quickly for the locally owned Internet service provider. I-Trap's official launch was only a few months ago, on Jan. 1, capping seven months of testing.Now Bright.net is marketing a glowing neon box that looks like it belongs in 2 Fast 2 Furious.

How i-Trap works

Bright.net's security system uses two sensors to gauge the effectiveness of a client's firewall.



SOURCE: Bright.net

Akron Beacon Journal

I-Trap is built to monitor network traffic for a host of hacker attacks. It works with existing security hardware and software, so the system isn't as costly as other systems, said John Clarke, general manager of Bright.net.

The initial installation ranges from $650 to $1,000 for a small to midsized company. Monitoring runs from $85 to $385 a month. Many competitors, on the other hand, could charge thousands of dollars for similar services, the company said.

Bright.net's employees also watch each client's network traffic and notify the company's network administrator if anything out of the ordinary occurs. What's defined as ``ordinary" is based on rules that each company sets up when i-Trap is hired. And the system can adapt on the fly.

I-Trap uses two sensors -- an Intrusion Detection System and Attack Detection System -- to relay data back to the main futuristic-looking box.

The sensors sit on both sides of a company's firewall, which lets data into or out of an internal network based on preset rules. That positioning is what sets i-Trap apart from its competitors, Desberg said.

Collecting data on both ends lets network administrators see how many hackers are trying to get into their system, and then compare that to what the firewall stopped. I-Trap itself doesn't block anything. The idea is to gauge the effectiveness of a company's security measures.

``Basically, we're baby-sitting a customer's firewall," Desberg said. ``It's the `I've fallen and can't get up' (device)of firewalls."

John Reinmann, president of Area 51 Consulting, said he doesn't understand why a company would need an outside service to monitor its firewall.

``Basically, it's not trusting your firewall, and I can agree with that. But my question is why? Why not just use the (monitoring) tools in your firewall?" he asked.

But Desberg said while most firewall programs generate such data, the reports are hard to read, even for IT specialists. I-Trap compiles that information into an easy-to-understand list that's available in real time on its Web site and stored forever.

That information can help IT departments investigate future attacks by looking at intrusions that didn't make it past the firewall. Other security companies typically keep that information to themselves because the intrusions didn't immediately harm the company's network, Desberg said.

That user-friendly monitoring is what Pete Kruft likes most about i-Trap -- along with the low price.

``It's opened my eyes to things that I didn't know were going on in the background," the network administrator for Barberton Citizens Hospital said. ``It's easy to check stuff."

Intrusion detection systems like i-Trap are in demand these days because Web-based attacks aren't in short supply.

In 1999, Carnegie Mellon University's CERT Coordination Center said 1,756 computer intrusion investigations were opened, 924 were closed and 54 ended in convictions. In 2000, 2,032 cases were opened, 921 were closed and 50 resulted in convictions.

Many attacks aren't reported, and CERT studies show intrusions are becoming more sophisticated with time.

The Internet security center also recorded 417 network security vulnerabilities in 1999. By 2002, there were 4,129 new ones.

``Most hacking attempts are not malicious. They want to control your server or hide," Clarke said. ``They want to use your resources to send out spam."

A firewall is a company's -- as well as an individual's -- first defense. And i-Trap could be the second.