

# CREDIT UNION TIMES

## Security Vendor TriGeo Aims to Form a NATO-Like Protective Alliance

2/3/2010 By Marc Rapport

Clients of TriGeo Network Security Inc. are given a small box, about 650 rules to live by and membership in a community that contributes to the enhanced internal and cyber protection of all, its chief spokesman says.

Those rules are the correlations of specific kinds of network activity—from simply playing solitaire to an attempted visit through a firewall from a computer based in a suspect country—into alerts (and later, compliance reports) for the people who need to know but have a lot of other things on their plates.

"Our target market is the small to medium-size businesses that do not have the luxury of large security operation centers staffed with professional security analysts. They feel a bit isolated and that they are on their own," said Michelle Dickman, president/CEO of the Idaho-based provider of network security to clients that include hospitals, insurance companies, electrical utilities, grocery retailers and about 200 credit unions.

"When a customer buys the TrioGeo SIM technology, they actually join a community," Dickman said, a community served by what the company calls its NATO-5 concept.

"The name is drawn from the fifth article of the NATO alliance, which states that 'an attack on one is an attack on all,'" Dickman said. Using client input and the work of her own staff of cyber security and network specialists, correlations (or rules) are created and distributed to the client community for deployment through her company's TriGeo SIM device.

The device continuously monitors activity and provides real-time log analysis that can actively respond by blocking IP addresses from entering the network while alerting key personnel through e-mail, cell phones, pagers or PDAs, the company said.

Shipping with more than 650 prepackaged rules already installed is a differentiator, she added, noting as an example one competitor she said ships with 13 correlations "that they want you to clone and use to write your own. Our competitors want you to write your own or pay their professional services to do that. We went the other way. We provide them free of charge as part of our support service."

And although she sells devices, the approach goes well beyond hardware, Dickman said. "Network security is a process not just a product," she added.

That philosophy is shared by Alan McHugh, manager of information technology at \$207 million U.S. Postal Service Federal Credit Union in Clinton, Md.

"Security is not just a department of IT. It has to be a company-wide policy, and if you have a breakdown in any of those, you might as well not have anything," he said.

McHugh said the TriGeo system has been useful in handling both the apparently mundane and potentially sinister. Someone playing solitaire on the network, for instance, gets the game shut down and a pop-up window from IT telling then to quit playing games at work. IP addresses from places where his members normally wouldn't be—such as Latin America, Africa or the Far East—also draw instant scrutiny.

McHugh said he also likes the USB defense feature, which allows him to ensure that only the appropriate user—for instance, the CEO—has the PIN and access to use that specific external device on the system.

"Credit unions have to look really hard at the way people can access information, can access your system, and you have to think about inside problems as much as outside these days," McHugh said, noting that many of the large corporate security breaches of late have been inside jobs.

He said he regularly participates in sharing the adjustments he's made to rules in his system with other credit unions. He's also a member of a CUNA list serve that shares IT security information as well.

"Me sharing information with them is not going to hurt my business, and we can all share our resources. It's a beautiful thing, because I don't have to reinvent something or delve too far for an answer that somebody already has," McHugh said.

Dickman said she sees that attitude a lot.

"While operationally they're not that different from community banks, credit unions will share information with each other in a snap in ways that banks won't. Things there are extremely competitive," she said.

The TriGeo CEO can rattle off example after example of ways that her clients have thwarted potential problems—such as a night security worker trying to log onto the network—and helped each other, including a Southern California credit union that developed a key cross-scripting rule. She also cited cooperation in heading off dangerous cyber threats.

Scott Schoolcraft said he's seen the results in his short time as a TriGeo user.

"With credit unions, that's just the way it is. We're happy to help each other out because we're not here to make a profit, but to help members, and that lends itself to helping out each other," said the vice president of systems at \$151 million Star USA FCU in Charleston, W.Va.

He credits his TriGeo device with quickly picking up the pernicious conficker worm in a computer on his network, at a teller station that was trying to send out spam. That was made possible, TriGeo's Dickman said, by quick distribution of a new conficker-fighting rule to the TriGeo customer network.

Schoolcraft said his new system also has made it possible for his two-person shop to now keep up with event logs at each location and end outsourcing of 24-hour monitoring of firewall activity.

"There was a little learning curve in the beginning, and it kind of helped that me and the girl who works for me had a little programming background—just to understand the flow of how it all works, but the training they give you is really all you need," he said.

"Once we had that, we were up and running."

[—mrapport@cutimes.com](mailto:—mrapport@cutimes.com)