

## Not just [SEM]antics

# Security-Event Management Solutions Offer Understanding, Protection

By MARC RAPPORT

*CU Times Technology Correspondent*

Spokane, Wash. – Here’s a new acronym for folks to learn in credit union land: SEM. It stands for security event management, and you’ll likely soon be seeing it routinely as IT security becomes a more complex, enterprise-wide event.

This service often begins with something as simple-sounding as an event log manager and develops from there to hardware/software combinations that detect prevent and provide alerts about internal and external hacks and attacks through a variety of communications devices to the people who need to know about them.

An early adopter of the systematic approach is Numerica Federal Credit Union in Spokane, Wash., which is using the Contego system from TriGeo Network Security of Post Falls, Idaho.

Contego centers on a hardware device that “consolidates, normalizes and correlates security events across your entire security environment, from the perimeter to the desktop,” says TriGeo’s CEO, Michelle Dickman.

A big part of that is making sense of the reams of hard-to-understand reports that devices like intruder detection systems (IDS) and firewalls generate as hackers and automated probes seem to endlessly try to find vulnerabilities and enter credit unions’ networks and eventually members’ accounts.

“It was hard, if not next to impossible, to keep up with and understand what all those logs from our servers, IDS appliances and firewalls were telling us,” says Kelley Ferguson, the network manager at \$450 million Numerica.

“The Contego solution integrates all that information into one interface where we can easily view all the logs without going from one PC to another, and in a form that’s much easier for us to understand, so we can tell what kind of intruder activity was going on and what we should do about it,” says Ferguson.

“It also lets us monitor in real time what’s happening throughout our systems, in all our branches and our network,” he says. “And it’s easy to understand.” Ferguson, by the way, carries some of the higher certifications in the IT security world, including Certified Information Security Systems Professional (CISSP). That level of expertise is not particularly common in the small- to medium-sized health services and financial institutions market that TriGeo is targeting with its Contego product, making its ease of use even more crucial to most of its clientele, Dickman says.

The Contego system, whose Version 2.1 has just launched this month, is easy enough to learn that its installation and deployment is done remotely by Web and telephone training, TriGeo says.

And its price, beginning at about \$18,000, is intended to make it affordable for the small to mid-sized financial institutions and health-services companies Dickman and her staff are targeting.

While Contego ships with the well-known Snort IDS device, the system is compatible with most IDS, virtual-private networks, network operating systems and other crucial hardware and software, Dickman says.

And like her client, Ferguson at Numerica, she stresses the pro-active approach Contego allows users to take toward IT security.

“Unlike other solutions that ‘play catch’ through passive integration and reactive measures, our solution pro-actively responds to security threats before, during and after a security event,” she says.

For instance, the system can block an IP address, disable an account, quarantine a workstation from the rest of the network or shut down a system, and then notify the powers-that-be through cell phone, pager or e-mail, Dickman says.

A good example of the breadth of SEM functionality comes from Dickman who recounts: “Our system alerted the manager of a local bank about 10 at night that someone was on the network, trying to log into accounts over and over again. He had the security company move the camera to the particular workstation where we tracked the activity to,

and saw it was the janitor.” Dickman’s story makes the point that security is and internal as well as exterior affair.

“Sixty percent of all attacks and breaches come from the inside,” she says. “Some are malicious, like Web site defacements or downloading a password cracker or keyboard logger, but also can be simply an unwitting employee just opening up an e-mail with a virus.

“Because Contego is watching all the network traffic, operating-system activity, audio/visual monitoring, IDS, firewall, routers and switches, we’re capturing events coming from the inside as well as outside.

“People need to remember: A firewall is not a brick wall.” Ferguson, the Numerica network manager, adds: “I like the analogy of a candy bar. Institutions spend hundreds of millions of dollars protecting the crunchy outside with firewalls and IDS, but it’s the inside, with all the soft caramel and things, that’s often even more unorganized, soft and unprotected.

“We now have a system that allows us to monitor in real time what’s happening inside as well as out.”

**“The Contego solution integrates all that information into one interface where we can easily view all the logs without going from one PC to another, and in a form that’s much easier for us to understand, so we can tell what kind of intruder activity was going on and what we should do about it...”**

**“It also lets us monitor in real time what’s happening throughout our systems, in all our branches and our network... And it’s easy to understand.”**