

Unified Threat Management

To Dream the Impossible Dream?

By Sharon D. Nelson, Esq. and John W. Simek
© 2006 Sensei Enterprises, Inc.

“Don't rush me sonny. You rush a miracle man, you get rotten miracles.”
- Miracle Max in “*The Princess Bride*”

Oh, but we do want everything instantaneously. In an IT world fraught with danger on all sides, we have clamored noisily for a security miracle. Where there is demand, a supply will emerge. Enter unified threat management, which heralds itself as the answer to all our security needs. UTM, almost unheard of outside the IT world in 2004, became gospel in 2005. UTM devices were rushed into production and the publicity bandwagons gathered full speed. As our selected quote above suggests, speed is not always desirable when it comes to IT security. Some of what we have seen is far less than a miracle, or perhaps, as Miracle Max suggests, a rotten miracle at best.

“Unified threat management” has become a buzzword phrase, one that would elicit blank stares from passersby on the streets, but which is getting lots of attention within the IT community. Unified threat management (UTM) came barnstorming into the IT security world in 2005, accompanied by promises of a one-stop shopping solution to all manner of security problems. It's no wonder we're so frantic. On January 19, 2006, the FBI released a study which noted that 90% of all business had suffered from a virus, spyware, network intrusion, online assault etc. attack in 2004 or 2005 and that the average damages amounted to \$24,000.

What is UTM? IDC defines UTM appliances as products that unify and integrate multiple security features onto a single hardware platform. These appliances must contain the ability to perform network firewalling, network intrusion detection and prevention, and gateway antivirus. Basically, one device layers together sophisticated software and hardware.

As always, when a thing seems too good to be true, it is worth taking a few wary steps backward and studying both the promises and the deliverables.

In a world of “blended threats,” unified threat management makes perfect sense conceptually. Most law firms have separate programs to deflect spyware, viruses, and network intrusions. They sometimes have multiple programs to perform the same function, particularly in the case of spyware. All of these programs must be purchased, licensed, managed, patched, updated, etc. And, as we all know, user error enters the playing field all the time - something doesn't get done and there's a problem, sometimes minor, sometimes catastrophic. One centralized solution sounds delicious and

economical. Oh, the joyful allure of dealing with a single vendor and a single point of administration in your network – it is an administrator’s dream.

Caveat Emptor. Those Romans really knew what they were talking about. UTM, while a great concept, is still pretty new on the horizon. There are three (at least) major issues. A UTM device might perform two or three functions admirably but be weak on the fourth. Many UTM solutions focus on perimeter security, ignoring the disgruntled and disaffected employees internally who cause so many of the problems. In fact, according to the FBI study referenced early, fully 44% of the incidents stemmed from someone inside the organization. Finally, the whole concept of UTM provides something that all IT folks hate – a single point of failure.

The converts to UTM are multiplying at a furious rate. IDC has reported that UTM is the fastest growing segment of the security market. It exceeded over \$100 million in revenue in 2003, a growth rate of 160% over 2002. By 2008, IDC projects that UTM devices will make up about 59% of the \$3.45 billion IT security market. Another 2005 industry study of IT managers found 50% of them “more” or “much more” interested in UTM solutions than they had been in the preceding year. More than 60% were seriously considering using a security appliance for multiple functions.

How much do these little bundles of joy cost? They can come for as little as \$1,500 for the small business models. Most companies offer a dizzying array of models meant to span the gap from major enterprises to very small businesses. The higher end models may cost up to \$70,000. One of the industry leaders, Secure Computing, says the base pricing on all eight of its models provides its customers with:

- A network layer stateful-inspection firewall
- An application-layer firewall with integrated IPS
- Controls for XML/SOAP traffic, IM, P2P, Spyware and Phishing traffic
- IPSec and SSL VPN termination for client-based or clientless VPN access
- A high speed, never-been-compromised SecureOS® operating system protected by patented Type Enforcement® technology
- Free web-based training
- Optional classroom training
- 24X7 technical support

Most companies now offer different suites for different needs intended to scale to the proper enterprise level. Some of the software is optional and may be selected as an opt-on module. For instance, if you like the anti-spam solution you have, you may “deselect” that when you purchase a UTM solution. UTM devices may also help with Sarbanes Oxley compliance by providing anti-spam, antivirus and content filtering software, as well as software designed to report who accessed data and when. Clearly, this is a good marketing tactic as SOX has many a company quivering in fear that it is not in compliance.

Who are some of the leaders in this brave new world? They include Fortinet (often called the industry leader), ServGate, Barrier1, Check Point Software, Internet Security Systems, Symantec, LokTek, Secure Computing, WatchGuard Technology, Network Box and Cisco Systems. To no one's surprise, Microsoft has jumped on the bandwagon too.

Without question, the assaults on our networks are painful, causing monetary damage, wasting bandwidth, draining productivity, and sometimes resulting in outright sabotage. Managing individual defenses to these assaults is labor intensive and costly. UTM devices provide an excellent start at combating security demons in an integrated way. But as one very candid manufacturer admits, no threat management software is 100% effective, 100% of the time." Sad but true. Even though UTM devices are often updated several times a day, there are still no true guarantees. And read those warranties carefully – they tend to exonerate the vendor in many real-life situations. What good is it to you if you have the latest and greatest in the UTM world but your data is gone? If your contract doesn't allow recovery of damages (first and third party), you may really be up the river without an oar.

Remember, once again, that unhappy employee of yours. One manufacturer trumpets the virtues of its UTM solution by saying "it allows one person to manage Internet threat protection for your entire network from one PC." Hardened skeptics that we are, given what we do for a living, we read that to say "your entire network security is in the hand of a single person who might sell you out or take revenge for some slight, real or imagined."

Another manufacturer has a tag line for its product: "the end of vulnerability." Forgive us if we shake our heads with resignation and cynicism. The bitter truth is that there will never be an end to vulnerability in IT security. There will never be a light at the end of the tunnel because the evil-doers of the world will continue vigorously to construct more tunnel.

It is tremendously difficult to gauge the worth of many of the UTM solutions because they simply haven't been around long enough. Of course, if you believe the advertising copy, everything is hunky-dory with all of them, but we have all become battle weary veterans of Madison Avenue and know the sad truth is that ad copy and reality rarely have much in common.

Companies have been so eager to scarf up UTM dollars that they are moving way too fast, sometimes stacking software with known vulnerabilities on top of software with known vulnerabilities. This is like building a fortified city and graciously leaving the key in front of the gate. Remember Miracle Max? "You rush a miracle man, you get rotten miracles."

The rotten miracles may naturally shake out as the industry shakes out. The Advisory Council, in a March 2005 issue of *Information Week*, suggested that most businesses thinking about UTM solutions be wary and let others do the preliminary bleeding. Few seem to be listening – the market is voting with its feet – but caution is really well-advised. The Council recommended studying UTM solutions and adopting them 2-4

years from the date of the article's publication, after the industry had a chance to repair its failures and companies not up to snuff had passed from the terrain.

So, let's take our miracles a bit more slowly. No one wants to be victimized by rotten miracles. The tried and tested miracle should be ready for most law firms in 2007. Patience is painful – but well advised.

The authors are the President and Vice President of Sensei Enterprises, Inc., a computer forensics and legal technology firm based in Fairfax, VA. 703-359-0700 (phone) 703-359-8434 (fax) sensei@senseient.com (e-mail), <http://www.senseient.com> (web site)