

August 14, 2006

UTM (D) Evolves

Opinion: The next-generation version of unified threat management is a little less unified.

By Larry Seltzer

For many businesses, especially smaller ones, the whole idea of UTM is an unambiguously great one: one box that can protect the network against just about all manner of threats.

It's relatively cheap, it's relatively easy to set up and administer, it protects the entire network, there's tons of competition, and there are plenty of options (although there is less competition since Symantec gave up not too long after launching its well-regarded product line.)

But there are problems with this sort of product, especially for larger companies. It's not uncommon for a company considering more gateway protection to already have a solid firewall in place. It must seem like a scam to have to buy a new firewall in order to get the other kinds of protection.

In fact, one could make the case that the firewall, at the low end, is well-enough understood and proven that it has become commoditized. At the higher end things are more complicated, but UTM is not a major issue in such markets.

This is why some have been arguing in favor of partially "de-unifying" the UTM. It's the classic convenience versus flexibility trade-off, with some "best of breed" arguments thrown in.

Take it to its logical extreme and you completely unravel UTM, but that wouldn't be logical for SMBs (small and midsize businesses). Clearly, at some level of company size and complexity, simplicity is more important than best of breed, and vice versa.

This is why Trend Micro is starting a new line of un-UTMs called the InterScan Gateway Security Appliances. It's the content-oriented parts of UTM in a box—anti-virus, anti-spyware, anti-spam, content filtering and URL filtering—and it protects HTTP, FTP, POP3 and SMTP. These aren't the be-all and end-all of Internet protocols, but they're certainly the Big Four.

Trend uses the term SCM (Secure Content Management), which tries to put the emphasis on "Content" as opposed to "Unified." It's targeted at medium-size businesses of 100-1,000 users. It also throws in a desktop scanning capability that gives a redundant second scan to the desktops

on the network. It also includes Trend's Outbreak Prevention Services, which download mitigating configurations, such as port blocking, in cases where a signature may not yet be available.

I like this as a compromise for such businesses. The convenience, for the physical network, for the administration and for licensing, is a major strength of UTM, and it is for SCM too. Many companies in the 100-1,000 size range will be able to administer a (for example) Cisco firewall and the Trend box themselves, but many will need a consultant anyway.

Symantec's retrenchment notwithstanding, we're in a golden age of security appliances. Companies of all sizes are offering products with security sourced from everywhere, including the open-source community. All of this competition should make things better for customers in the long term, driving prices down and increasing the power and accessibility of network protection. UTM, SCM, who cares.

Security Center Editor Larry Seltzer has worked in and written about the computer industry since 1983. He can be reached at larryseltzer@ziffdavis.com.

Reprinted from eWEEK, August 14, 2006 with permission from Ziff Davis Media Inc.
©2006 Ziff Davis Publishing Holdings Inc. All rights reserved.

