



# Cover story





## COVER STORY

# Give us this day our UTM



Danny Bradbury

As malware becomes more sophisticated, Unified Threat Management systems must also evolve, but without losing touch with a major selling feature: simplicity. **Danny Bradbury** thinks outside the box

Here's the gospel of network security: in the beginning there was the firewall, and the firewall was good.

Unfortunately, in the IT world as in the Biblical one, things never stay simple. Firewall vendors, eager to differentiate themselves, started adding things to their products: a VPN (virtual private network) here, and perhaps a web content scanner or an intrusion prevention system there. Before you knew it, the firewall was doing all kinds of things outside its original remit.

Then, on the sixth day, an enterprising analyst at IDC noticed all this and said 'let there be unified threat management'. And that's how the new product category, like many others, was born.

## What's in a name?

If there was a patron saint of UTM (unified threat management), it certainly wouldn't be Greg Young, research vice president for network security at Gartner. He doesn't like the term (and not just because he didn't think of it first).

"You can't manage threats," he complains, adding that his company finally capitulated and started using the phrase to try and tease out a solid product definition and dispel some of the marketing hype coming from vendors.

Not even the manufacturers seem to agree on how the term should be used.

"I think we are better off simply calling our stuff 'threat management'," says Paul Judd, regional director for the UK and Ireland at Fortinet, arguing that the security tools in his company's appliances didn't need to be unified in the first place.

Fortinet, which includes a range of features such as content web filtering and traffic shaping in one box, wrote all of the software itself rather than sourcing it from specialist providers. "It increases performance, and it also benefits you from an application



**At the very least...a device should include the basic firewall, along with the VPN, anti-virus, anti-spam, and intrusion prevention system to be classified as a UTM**



## COVER STORY



Paul Judd, Fortinet

perspective," he says, explaining that users can better manage everything through a single console.

Tim Helming, director of product management at UTM vendor WatchGuard, calls his brand of product 'extensible threat management'. "Customers can turn on what they like, but they don't have to turn on everything," he says, describing his product's feature set. "It makes more sense for the customer."

### Cramming it in

Regardless of the debate around what is and isn't a UTM system, the need for more than simple firewall functionality is clear.

Years ago, ports were more readily mapped to applications, and understanding and stopping threats was a relatively easy task for a well-configured firewall. Today, multiple threats cross the network boundary unpredictably through different ports.

"They go after everything that's installed," says Patrick Walsh, director of product management and marketing at eSoft, which focuses on the SMB (small to medium business) market with its appliances.

"If you have one machine that doesn't have a current version of the adobe PDF plugin - that is going to get hacked."

SMBs are the only real market for UTM boxes today, Young asserts. SMB customers don't need cutting-edge functionality, and can merge low latency security applications such as firewalls and intrusion prevention systems together with others like antivirus and e-mail scanning that don't rely on very low latency behaviour.

At the very least, Young says that a device should include the basic firewall, along with the VPN, anti-virus, anti-spam, and intrusion prevention system, to be classified as a UTM.

"There also tend to be some other things that come and go," he says. Functions such as data loss prevention and anti-phishing may well find their way into such a box, but UTM appliances needn't have those to meet his criteria.

That's a lot to fit in one box, and in the enterprise space, he argues that very few, if any, companies have been willing to take the risk.

"There is convergence going on at the enterprise but they don't get the all in one that the UTM offers," he says, adding that 'appliance compression' creates three broad categories of product for large firms: IPS (intrusion prevention system) enabled next-generation firewalls, mail scanning functions aggregated into a single border security system, and finally anti-virus and URL content scanning security devices.

"You won't get them coming together [more than that] in the enterprise because they are very different buying centres, and you won't get one vendor that is best of breed for all of those."



**Devices should be very easy to configure, ideally by a non-security professional (because most small businesses won't have one)**



**The more features that you put into a single appliance, the more processing you need to handle the network traffic as it passes through the UTM system**

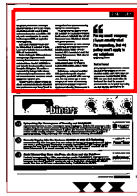
Some vendors would disagree, offering what they claim is UTM for the enterprise, but Young urges users to look beyond the same marketing hype that creates endless sub-phrases such as 'extensible threat management'. But WatchGuard's Helming thinks that the relevance to the enterprise is changing as the UTM category matures. He is already calling for closer integration between UTM systems and the systems management products that vendors such as HP, BMC and IBM Tivoli are targeting at larger businesses.

### Tailor-made for comfort

As UTM vendors eye larger customers, they are focusing on features that smaller companies may not be as interested in.



Tim Helming, WatchGuard



## COVER STORY

For example, Fortinet offers the ability to virtualise instances of UTM to suit multiple, virtualised servers. One virtual operating system may be running an application that only needs e-mail scanning, for example. Another may need VPN and application firewall capabilities.

Judd argues that customers can tailor the UTM appliance to support all of them. Large-scale virtualisation isn't something that SMBs will be interested in.

Another challenge to UTM manufacturers wanting to target larger customers is scalability. The more features that you put into a single appliance, the more processing you need to handle the network traffic as it passes through the UTM system. This problem is compounded by the larger traffic volumes experienced by enterprise customers, which will continue to increase as backbone network speeds in the enterprise grow.

These drivers have gradually phased out players putting multiple security applications onto generic servers, says Young. "It can't be done with general-purpose boxes," he says,

although CheckPoint's product marketing manager Bill Jensen disagrees.

The company strings together multiple Intel processors in a single box, and uses its CoreXL system to balance the load between the processor cores. WatchGuard also uses more generic processors.

"We recognised that the threat landscape is changing so dynamically that if we were forced to revise our silicon with every important shift in the market, it would take too long," Helming argues. "We'd rather be more nimble."

Nevertheless, the company uses a specialised processor for offloading cryptographic functions, which increases performance.

Fortinet uses a mixture of specialised ASICs (application-specific integrated circuit) with a generic CPU at the core, says Judd. That way, if a new type of threat emerges, it can handle the threat using software on the processor until product development allows for it to be encoded in ASIC hardware for additional speed.



**For my small company I know exactly what I'm expecting, but my policy won't apply to my neighbour**

Greg Young, Gartner

### Best of breed

Unlike Fortinet, Checkpoint chooses to source non-core components such as anti-virus from other vendors, which Young says is the more common theme in the UTM market. SMBs care more about simply getting the box to work than about the nuances of performance that can be gained from writing your own integrated software from the ground up, he says.



## COVER STORY

The tension between 'best of breed' and 'home rolled' beauty and systems is crucial. Fortinet isn't the only company that developed all of its security applications itself. eSoft did the same, and this was one reason that Gartner placed the company in its 'caution' category when evaluating the SMB UTM market.

And yet, Young gives Fortinet a 'strong positive', in spite of similar concerns about its ability to deliver a comprehensive set of features using home-baked code. Its high visibility and ability to deliver products to suit a wide variety of SMB scenarios makes it a winner, according to the analyst firm.

Checkpoint's Jensen maintains that the company's added value lies in its customer relationships. "The customer deals directly with us. Support and updates all come from us. It's not just an open source project that someone slapped on a box and called UTM," he argues.

### No size fits all

The importance of good customer relationships and support cannot be underestimated in the UTM market. Devices should be very easy to configure, ideally by a non-security professional (because most small businesses won't have one).

Pre-sales support is crucial: "Where we see people getting into trouble is with their sizing of devices," warns Young, pointing out that they put everything into an undersized box. "Then they have to go back to the vendor, buy a bigger box, and lose some investment." Channel partners are therefore an important part of the mix.

While UTM vendors try to push their way up into the enterprise, displacing what Young distinguishes as the next-generation firewall category, might they find themselves being squeezed by managed services providers in the SMB market? If all-in-one network traffic processing requires more computing power, some might argue that it

is best done by a hosted provider with more processing muscle.

Cash and experience-starved SMBs have already bought into managed security service providers such as Postini, for mail scanning and anti-spam services.

As firms like Symantec ready platforms for integrated managed security services, could hosted UTM offerings be far away? One problem could be customisation, says Young.

"In the cloud or upstream you have to take a fairly light touch on your traffic blocking," he says. "For my small company I know exactly what I'm expecting, but my policy won't apply to my neighbour."

As security vendors try to cram everything in the same box, the malware writers are thinking outside of it. Phishing, targeted attacks, trojans and worms are becoming more sophisticated, and doing their best to find their way through any open door they can find.

Small businesses with little or no expertise need all the help they can get - preferably in an all-in-one system with a simple interface. ■