

UTM

Fully armed

Unified threat management appliances are billed as a low-cost security solution. And they are no longer the preserve of SMEs. By Steve Gold

Contrary to what some industry experts claim, unified threat management (UTM) systems have been around in one form or another since the start of the decade. It's only in the past few years, however, that the technology has entered the mainstream IT security market, largely thanks to the development of relatively low-cost, rack-mounted appliances with high processing power.

These appliances can sit on the edge or at the centre of a company's IT systems and run a variety of IT security applications, including a stateful inspection firewall, intrusion-detection software and a blend of anti-virus, anti-spam, anti-spyware, and content-filtering applications.

As well as integrating traditionally separate security services into a single device, UTM appliances also offer streamlined access to IT security policies and reporting. From an IT manager's perspective, these devices are great time savers, allowing updates to be scheduled and initiated from a single console, while reports can be viewed and policy managed from one appliance.

Those are the pros; what are the cons? One argument against unified threat management is that IT staff cannot normally select which security applications they run on the appliance – most UTM vendors offer a selection of programs on a limited mix-and-match basis.

For most IT managers, however, this is a moot point, because UTM vendors tend to offer 'best-of-breed' security applications that also work together quite well. Astaro, a veteran in this sector, uses a combination of Kaspersky and open-source signatures for its virus protection, for example.

Another argument against UTM is that the appliances can only protect the network or company IT resource against known threats. Unknown threats require the use of a behavioural-analysis system such as Tier-3's Huntsman technology.

And then, of course, it's important to realise that a UTM appliance is designed to stop threats before they reach the company network – IT managers should still employ desktop anti-virus and anti-spyware protection on the desktop, primarily as the last line of defence.

According to Udo Kerst, senior product manager at Astaro, whose UTM lineage dates back to 2000, UTM appliances offer real value for money and ease of use in what is otherwise a complex IT security market.

However, he acknowledges that UTM is not for every company. "There is a space, in the higher-end market, where the technology doesn't fit," he says, although he points out that UTM appliances can also be used in parallel with third-party technologies, such as blended threat-prevention software.

But what about customers who are

looking for a specific brand of IT security software to run on a UTM appliance?

In Kerst's experience, most customers are not looking for a branded IT security offering but a best-of-breed solution that is flexible in terms of performance and scalability.

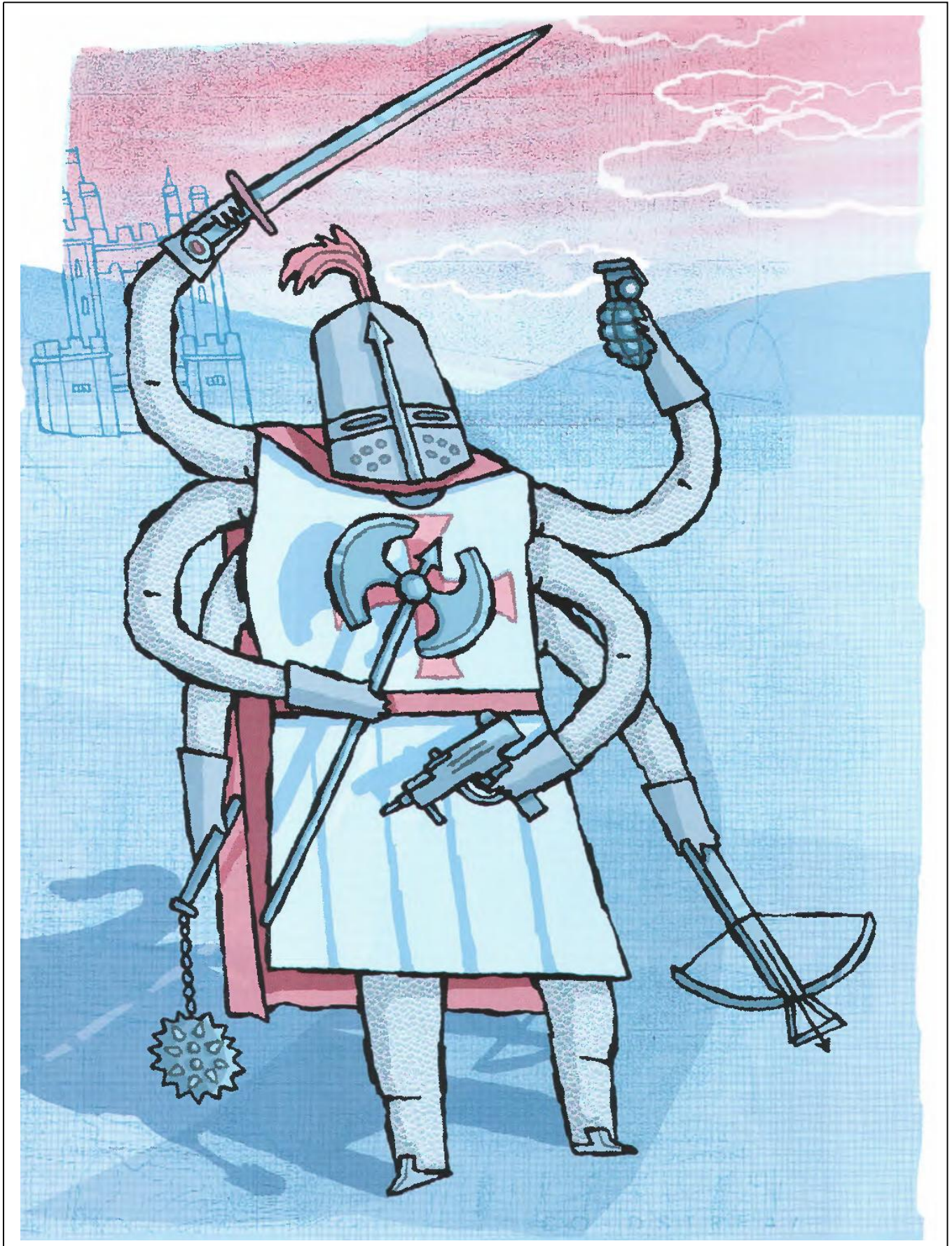
"Our approach is to offer customers a modular set of solutions based around a central set of protection such as firewall, intrusion detection and so on, to which up to three extra packages can be added – email protection, web traffic analysis and control, and email encryption," he explains.

Most UTM customers, he adds, take the central protection option and then add the extra packages as they look for extra levels of IT security.

Solutions for big business

Kerst predicts that, in future, UTM vendors will progressively develop appliances that can cater for larger organisations, perhaps as many as 1,000 or more, although servicing the needs of 2,000 users from a cluster of networked UTM appliances, he admits, is not going to be an easy task.

Over at Fortinet, chief marketing officer Richard Stienon says his company is already servicing the larger enterprises using the firm's FortiGate systems. These systems, which include firewall, VPN, anti-virus, intrusion prevention, web filtering, anti-spam,



UTM

anti-spyware and traffic shaping in their long list of protective applications, can be deployed individually or combined for a comprehensive UTM solution.

“There’s a lot more to UTM than most people think. If you use the right technology, you can extend UTM into organisations with as many as 1,000 users,” he says, adding that this is made possible by using very high power ASIC technology such as that seen in Fortinet’s network-based ASIC-accelerated enterprise offerings.

“You can also add other IT security technologies to the mix, such as behavioural analysis, to counter unknown threats, but these solutions tend to be hosted, rather than a standalone appliance,” he explains.

Stiennon says Fortinet is able to meet the UTM needs of SMEs and even large enterprises by taking a modular approach to the hardware aspect of UTM appliances. This is possible, he

If you use the right technology, you can extend UTM into organisations with as many as 1,000 users”

Richard Steinnon, chief marketing officer, Fortinet

says, because the FortiGate range is actually a modular security protection system that can be scaled up.

These high-end systems, he adds, are moving beyond their UTM appliance roots and into relatively new territory, since they can be interfaced with third-party security technologies.

Which is where the UTM industry gets interesting, because it’s clear Fortinet’s approach is evolutionary in that its UTM appliances are outgrowing their origins.

A new chapter

This evolution isn’t just confined to the UTM appliance market, but has also reached into the software industry, as witnessed by Check Point’s decision in February this year to move into the mid-range UTM appliance market.

In many ways, the development of the Check Point UTM-1 series mirrors what has happened at Fortinet, namely the development of a single UTM appliance

CASE STUDY Liverpool Direct

Liverpool Direct is an unusual hybrid company. It was set up as a joint venture between Liverpool City Council and BT to help the council transform the way it provides its public services. The company is developing a range of e-government and interactive facilities to make public services such as revenue and benefits, training and social services more accessible.

Liverpool Direct provides connectivity and ICT services for the council, its partner organisations, local schools and city learning centres.

Security is a critical component of the organisation’s operations and the company’s deployment of Fortinet technology saw it earn the British Computing Society President’s Award for Investment in Information Security in 2006.

Liverpool Direct needed a large-scale security infrastructure to protect its network. The primary requirement was to secure the council’s corporate data functions – including HR and payroll – from web-based attacks.

Mark Orford, the organisation’s head of technical architecture and strategy, led the project. “We



UTM: protecting Liverpool’s educational IT resource

recognised the need to upgrade our dated security systems to protect against the increasing danger from web-based threats,” he says.

An extra element of its network requirements that Liverpool Direct looked to secure was its ICT services to local schools. This required a flexible security platform that could ensure each connection would be constantly protected against a range of threats.

After a technical and commercial review, Fortinet’s UTM network security platform was chosen for web-based content filtering on the basis of its high levels of protection and low total

cost of ownership. Liverpool Direct deployed a range of Fortinet multi-threat UTM appliances, including the FortiGate-800, across the entire council’s network.

The vendor’s UTM technology is also helping Liverpool Direct meet its duty to schools by blocking inappropriate email and web content to its students. The system is credited with halting more than 66,000 web pages in December 2006. A similar UTM system also ensures clean content is provided to a number of businesses in the area.

FortiGate-500A appliances were originally deployed across the city’s school networks primarily for their web-filtering capabilities, but due to their multi-layered nature, Liverpool Direct quickly started using the anti-virus and SMTP email scanning capabilities as well.

According to Orford, educational establishments are increasingly reliant on technology. “But with security policies differing from school to school and age group to age group, this can be a management nightmare. Fortinet enables us to protect the network more effectively,” he says.

UTM

into a rack-mounted multi-card system that caters for hundreds of users, even up to 1,000 users or more.

Check Point's UTM-1 range distils the company's unified security architecture into a modular rack-mounted appliance that can be integrated with the firm's SmartCenter/Provider-1 technology.

Nick Lowe, Check Point's regional director, says that what is driving the UTM market is the growing need for simplification of IT security technology. "This need isn't just confined to the SME sector. Even the largest enterprises are looking for it, which is why we've developed our UTM-1 range," he says.

What's interesting about Lowe's approach to promoting the new UTM-1 systems is that, like Stiennon, he acknowledges they move beyond the usual UTM appliance segment and into the enterprise end of the market.

"The UTM-1 series are very high-power systems that are future-ready. As we develop new IT security applications, they can be loaded on to the UTM-1 platform without any degradation in overall performance," he says.

This is something that's not possible with pure UTM appliances, he explains, owing to their relatively simple processor architecture.

Lowe adds that Check Point took the decision to enter the UTM appliance market when it realised that a growing number of large companies were looking for the IT security firm's Smartdefense pre-emptive security technology but didn't have the skills to monitor and update the software on an in-house basis.

Maintaining performance

"While we were planning the UTM-1 series, I looked at the other UTM offerings in the market and soon realised that there were clear performance penalties as you start to switch on more features," he says.

This degradation of performance, he adds, is clearly seen on peer-to-peer

Where is UTM headed?



We put this question to **Nick Lowe**, regional director of Check Point, which moved into the heightend UTM market this February with its UTM-1 range of systems.

UTM, he says, is moving beyond its appliance origins and into a multi-processor and modular world that will see solutions extending into the enterprise marketplace.

The UTM-1 series was developed to cater for the growing number of applications that need high levels of security, according to Lowe.

"These include VoIP, instant messaging and peer-to-peer applications, which are relatively new to the IT security arena," he explains, adding that a growing number of enterprises are looking for a component-based appliance solution.



Geoff Sweeney, CTO at Tier-3, the behavioural-analysis IT security software specialist, also sees UTM as evolving upmarket, but with the proviso that such

systems will increasingly interface with third-party security systems outside of the UTM space.

"I think you're going to see a number of changes in the UTM market in the next few years, with vendors offering solutions that cater for larger

enterprises, as is already happening at Fortinet," he says. "The problem with scaled UTM, though, is that no matter how you look at it, even the most innovative UTM system cannot protect you against all threats."

Sweeney says, despite this limitation, he understands where companies such as Astaro and Fortinet are coming from and sees a healthy future, with next-generation UTM appliances interacting fully with third-party security systems.

"Ideally, I'd like to see a scalable UTM appliance that interfaces with our Huntsman behavioural analysis technology. I'd see that as a logical evolution of UTM," he says.

The main issue with UTM appliances, in Sweeney's opinion, is that they cater for a segment of the market that doesn't have the knowledge or resources to monitor and maintain a larger-scale IT security system on a daily basis.

"That's where UTM technology has its niche and it's a good one," he says. "In the future, I think you're going to see a lot more hybrid UTM technologies that, when you get down to basics, are not really pure UTM solutions." Sweeney adds that a blurring of the boundaries between UTM and other IT security technologies is a logical progression.

applications, which is why the UTM-1 series can place limits on such services, while controlling what they do at the same time.

"On top of this, we realised that UTM systems needed to be deployed by people without many IT security skills. This is why we developed UTM-1," he says.

While Check Point is moving into the UTM marketplace after several years of success in the enterprise security segment, a number of vendors are moving into the periphery of the UTM market, with alternatives to the traditional appliance.

BigFix's strategy is to install an endpoint server and console on a company's network, which then acts as a gateway between its own headquarters systems and a software agent that sits on users' PCs within the company.

This set-up is similar to a UTM

Larger enterprises need multiple appliances, and this goes beyond what UTM is currently capable of"

Yuval Ben-Itzhak, CTO, Finjan

UTM

appliance, but with the key difference that the platform appliance is in constant contact with BigFix's headquarters systems for information on patches and updates and share this data with each PC on the company network.

Modular approach

Colin Gray, vice-president and MD of BigFix, says the company's platform is modular, allowing companies to select only those services they need, rather than going down the one-size-fits-all approach of traditional UTM appliances.

"In a sense, the BigFix platform is an evolution of UTM on a modular basis," he says, adding that, while UTM technology protects against known threats, BigFix's platform can also protect against unknown threats as they develop, thanks to the firm's ongoing threat-analysis programme.

Gray acknowledges the position that UTM appliances have in the market. "Unified threat management is a recognition of the fact that there is a need for a single-console security system," he says. "The key issue with UTM is that it cannot normally grow with an enterprise. There will come a point when their existing UTM system needs to be replaced," he says.

According to Gray, one area that UTM appliances cannot normally cover is policy enforcement. "There are other solutions that cater for this need, so it's important to realise the limitations, as well as the advantages, of UTM technology," he adds.

Over at Finjan, meanwhile, which describes itself as a pro-active web security solutions vendor, Yuval Ben-Itzhak, the firm's chief technology officer, says UTM appliances are ideal for SMEs of up to 800 users. Beyond that, they simply cannot scale up effectively.

"The problem is the load on the box. Even if you have multiple processors, you are going to hit a processing limit," he says. "Larger enterprises need multiple appliances, and this goes

beyond what UTM is currently capable of."

Limited possibilities

Ben-Itzhak adds that, while some UTM vendors claim to service the IT security needs in relation to VoIP and peer-to-peer traffic, unless the system is a hybrid one, then it cannot deal with these kinds of threats.

Having said that, Ben-Itzhak does acknowledge that some situations, such

as branch offices, do need a UTM appliance that can interoperate with an enterprise's main security platform.

"That platform is typically supplied by two or three vendors when you are talking about an enterprise with 1,000-plus users," he says. The problem with using a UTM in a branch of a larger enterprise, he adds, is that the head office cannot set the security rules for the branch. "That is UTM's main limitation in my opinion," he concludes.