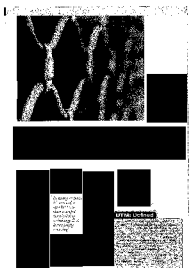
Publication: Computerscope
Date: Thursday, May 18, 2006
Page: 39
Extract: 1 of 6
Circulation: 9.681
Author:
Headline: One for all



One for all

Has unified threat management matured to become a viable weapon in the enterprise security arsenal? LESLIE FAUGHNAN examines the issues

At least one part of the trouble with three letter acronyms is that they are ugly, confusing and often ambiguous — but frequently useful if only to avoid repeating mouthfuls of jargon. So Unified Threat Management, the latest addition in the field of security, is beginning to be known as 'UTM' and in this article we will use the abbreviation for convenience. But although the underlying concept is in fact now behind an ever-broadening range of mainstream products, many experts are more than dubious about the value of the term.

See the inset panel for a closer definition of UTM.

Devices

UTM devices range from the simplest, plug and play out of the box units to more sophisticated appliances that offer a high degree of 'tuning'. All of them have built-in processors and data storage capacity (even hard drives at the top end) for the performance rules, virus definitions and signatures, banned URLs, etc. which are the basis of their effectiveness. These are updated automatically and frequently over the Internet, as often as hourly in some cases, by the hardware vendors or their partner supplier of the antivirus and other active applications in the device.

An UTM appliance is in fact a combination of product, with an initial purchase cost, and an annual subscription service for the updating. The principal appeal to the market is very clear: the all-in-one simplicity of an appliance with no user input required and at attractive price points compared to best-of-breed software or other alternatives.

Challenge and change

"In a way it's a bit mystifying why the industry suddenly discovered the 'unified' approach to security — except as a popular marketing term," said Tony Redmond, the Irishman who is Hewlett Packard vice president and security strategy head.

"We have been relying for some years on traditional strong, layered perimeter defences that still deal with perhaps 90% and more of the issues. The big change, the big challenge and increasingly the focus of development work is dealing with transient connections by trusted insiders. Mobility, teleworking, multiple portable devices and multiple protocols have all introduced new complexity."

The value of the automated system built into a single device is that it guards against simple mistakes, Redmond believes, including failure to update in time or correctly. "So it certainly has a value for smaller businesses. But the key word is 'integrated' with coherent systems and policies across all of the organisation, so you would have to be sceptical about un-managed

Publication: Computerscope
Date: Thursday, May 18, 2006
Page: 39
Extract: 2 of 6
Circulation: 9.681
Author:
Headline: One for all

devices in a large scale enterprise. But UTM devices may certainly have a place, because the threats range from low level and generic to very sophisticated and targeted attacks on specific types of organisation, like banking or government. The principle of a layered set of defences will still be valid and devices will have a role in the front line."

Integrated intelligence

Networking giant Cisco with its 'Self-Defending Network' strategy has been for some years building more and more intelligence and security into all of its network devices. Its Adaptive Security Appliances may sound like UTM but the resemblance is simply in the general approach of putting more security systems into a new generation of smarter boxes. "You can save a lot of costs and greatly simplify management by standardising on a single platform," explained John Stone, Cisco chief technical officer of Cisco Systems Ireland. "Every organisation today has to configure the firewall, VPN, intrusion prevention and anti-everything. So in fact there is a real danger that security will become weaker because of management issues. In that context, the growth in the market will certainly be for consolidated platforms with more functionality at reduced prices."

At the SME level, he accepts, automatic appliances will probably be adequate for most businesses. But at a higher level there are issues of scalability for huge traffic volumes. "We are also concerned about Day Zero attacks which tend to be directed against larger organisations. Something new and smart tends not to be aimed at the general run of SMEs. So you are looking at the constant development of multi-layered, pro-active defences that can instantly identify threatening behaviour in-line. Even dynamic signature update releases—as quickly as 15 minutes after a new threat is spotted—are not good enough at this level."

Required depth

Networking vendor, 3Com also shares the view that enterprise-level security requires more depth than UTM appliances can offer. "There is certainly a trend towards ever-smarter boxes, and we are in that space with Tipping Point intrusion prevention and detection devices," said Ray O'Connor, 3Com country manager. "But overall the UTM approach has to be seen as more of an SME or branch level solution to avoid the problems of multiple devices and all of the management issues. In many respects it's more of a market term than a useful description of technology that is constantly evolving and being designed into all sort of networking equipment from the chip up. We are developing network switch technology with a range of security defences built in, for example. On the Tipping Point side, you are talking about inspection of every data packet traversing the network but with no negative impact on performance."

He suggests that larger organisations will have rack-mounted arrays of such devices, like blade servers, to handle vast traffic volumes of data throughput at up to optical fibre speeds if required. Larger networks and WANs will have segmented security protection. On the other hand, he accepts, in many organisations the Internet gateway can be seen from a security point of view as just one channel and not a very fast one at that. "A smart appliance at that point is certainly a valid solution. But you also have to look at the overall design of the network because, of course, it is not the only potential channel for threats."

Update strength

One of the leaders in Internet security is Check Point, which has confidently added UTM appliances to its range of technologies in recent years. "In the beginning our solutions were software and server based but round about the turn of the century we began to look at smart devices and partnered, for example, with Nokia well before the UTM market took off." Niall Moynihan is country manager for Check Point in Ireland and is quick to add that his company's solutions span from entry level ADSL-ready appliances all the way up to systems for global multinationals.

Although it has extended into hardware devices, it is fair to say that Check Point's reputation for world class security software is still its market strength. This is reflected in the fact that it continues to be the security system partner of choice for other hardware manufacturers. "One of the great strengths of the UTM approach is that security updating is automatic and remote, making it ideal for smaller sites. Our annual subscription for this service is at a standard 15% of the original investment," said Niall Moynihan. He points out, however, that partners and vendors may add another few points for service and support so that the range for almost all UTMs is between 15-20% annually.

Licence advantage

In the Irish market, Topsec Technology is a distributor for some of the leading UTM brands such as Zyxel and Watchguard. "The arguments for UTM are really very straightforward and practical," said David

Publication: Computerscope
Date: Thursday, May 18, 2006
Page: 39
Extract: 3 of 6
Circulation: 9.681
Author:
Headline: One for all

Girvan, Topsec's channel manager, "and that is why the products are gaining so rapidly in popularity. You have a high level of smart protection in a single box, minimal management if any and you pay just a single annual charge for an automated and very frequent updating service. Most companies today are paying multiple licence fees per user for their antivirus and other security software, for example. With a UTM box the manufacturer has already negotiated a block licence and the actual security applications are likely to be from world leaders anyway, like Brightmail for e-mail filtering."

As he puts it, "There have been some serious hormones added into the processing power of these boxes recently. So the smaller Irish organisation is getting the same levels of security protection for perhaps 100 users as it has been from multiple 'best of breed' specific solutions. In practica terms it may often be higher because the dangers of incorrect and inefficient implementation have been taken away. It is also a good value solution. Interestingly, we have particularly noticed early adoption by professional services firms such as lawyers, accountants and so on."

Branch app

The general view that UTM is principally for smaller organisations is endorsed by Darren Lawlor, manager of Unit 4 Security Solutions. "We see UTM devices as very much part of the way forward in security, particularly with the proliferation of network access points, from teleworking to a growing range of mobile devices. So much so, in fact, that we carried out exhaustive testing of different appliance ranges before choosing Fortinet as our UTM brand of choice."

Lawlor makes the point that although a major strength of UTM devices is the fact that they are effective with no user management, there is also a place for them as part of a managed strategy. "In that context we see them usefully deployed in many situations as access security devices. But we manage the updates and configuration remotely as part of the managed security service, especially in relation to ensuring that all policies are consistent throughout the network. Policies can also be changed to match changing circumstances rather than accepting what comes out of the box."

This is in fact the consistent view of most security experts, reiterated by Michael Conway, managing director of Renaissance Contingency Services, "What we are all aiming for is integrated threat management across all of the network and devices in an organisation. We work with Sophos, one of the world leaders in IT security, which has for some time recognised that security had to move from the traditional server and network based systems out to all of the client devices and endpoints. What is still important is that security be centrally managed, especially in larger and more complex organisations, to ensure consistency as well as effective performance - 'integrated' in other words."

But now we are talking about a high level of skill sets, he points out, which may not always be available within even quite large organisations. That is one reason why the trend worldwide is towards integrated threat management with a single 'console' to manage centrally the core security of all elements of IT infrastructure. "In that context, UTM devices do indeed work out of the box, so they are a large part of the solution for the simpler and usually smaller organisation. But they work even better when they are managed and tuned to your specific — and changing — policies and security needs."

Encryption blind

IT equipment distributors, Commtech, has been specialising in network security solutions for some years and includes leading names in its portfolio such as Sonicwall, Cyberguard, Barracuda and others. "We have seen rapid growth in recent years in all sizes of organisation with the spread of broadband and the recognition, for example, of the crucial importance of firewalls," said Justin Owens, director in charge of the Commtech professional services team. "The good thing about UTM, especially in smaller businesses, is that is simplifies security so that the protection of the applications in the box will actually be fully implemented. You have best-of-breed solutions in the devices and in essence an SME can protect itself against more than 80% of the threats for perhaps less than 20% of the costs of comparable software solutions at network server level."

He points to one snag that does affect some sections of the market, "A UTM box cannot see inside the data packets if the traffic is encrypted—yet encryption is common in many kinds of online transactions, from banking to credit card acquisition to supply chain relationships. But the appliance approach still holds good, just that now you move a step up to specialist devices such as Bluecoat for web filtering."

Configuration boon

That best of breed specialist device approach is working well for Galway-based Copperfasten and its highly successful Mail Firewall Appliance, launched in 2004. "It does what it said on the box—cleans your e-mail and protects against all e-mail-borne threats as well as filtering out spam," said sales manager Ronan Kavanagh. Entry level is about ten users, he explains, but one UK university is using Copperfasten to serve

Publication: Computerscope
Date: Thursday, May 18, 2006
Page: 39
Extract: 4 of 6
Circulation: 9.681
Author:
Headline: One for all

35,000 users on its network. "We are very much part of the device-based security market, but perhaps a step up from all-in-one UTM boxes which almost by definition cannot match the calibre of a dedicated device. There is a modest amount of initial user configuration required, maybe 30 minutes or so. But after that the solution is fully automatic as far as the user is concerned, but with AV updating as often as hourly and intelligent self-configuration within the box as the threats evolve and change."

BT Ireland sees the growth of UTM devices from two perspectives, according to security sales specialist Dave Burke, "As a major ISP, we have a constant interest in the protection of our customers. As technical consultants and a managed network services provider, we are constantly evaluating security issues and the changing threats. The notion of consolidating security measures applies at all levels, from enterprise to SME to personal user. The benefit of UTM is that it does that and does it simply at the Internet access point.

'In many respects it's more of a market term than a useful description of technology that is constantly evolving'

The traditional best of breed server-based software is still the top-level solution. But it's multiple and therefore difficult to manage." On the other hand, he points out, it is not an either/or question: UTM appliances have a role at many network levels and end points as a valuable constituent part of an overall security strategy.

Complexity relief

Overcoming complexity is probably the universal theme from experts we have talked to about UTM. There is unanimous acceptance that more and more intelligence in the boxes that run our networks is essential and also that smaller organisations must be offered automatic solutions to guard against the growing volume and variety of threats. "There is also the question of the evolving and multimodal ways in which we communicate with our networks and the Internet," as security consultants Sean O'Connell of CA Ireland points out, using VPNs from different portable devices, transient locations and so on. "Integrated threat management, whatever term you use, is the important thing. Consolidation into one central point of view and control is the objective, with uniform management and implementation across perhaps hundreds of locations. But the key to any serious security solution is that it is multi-layered. Hardened boxes and firewall appliances have their place in the front line."

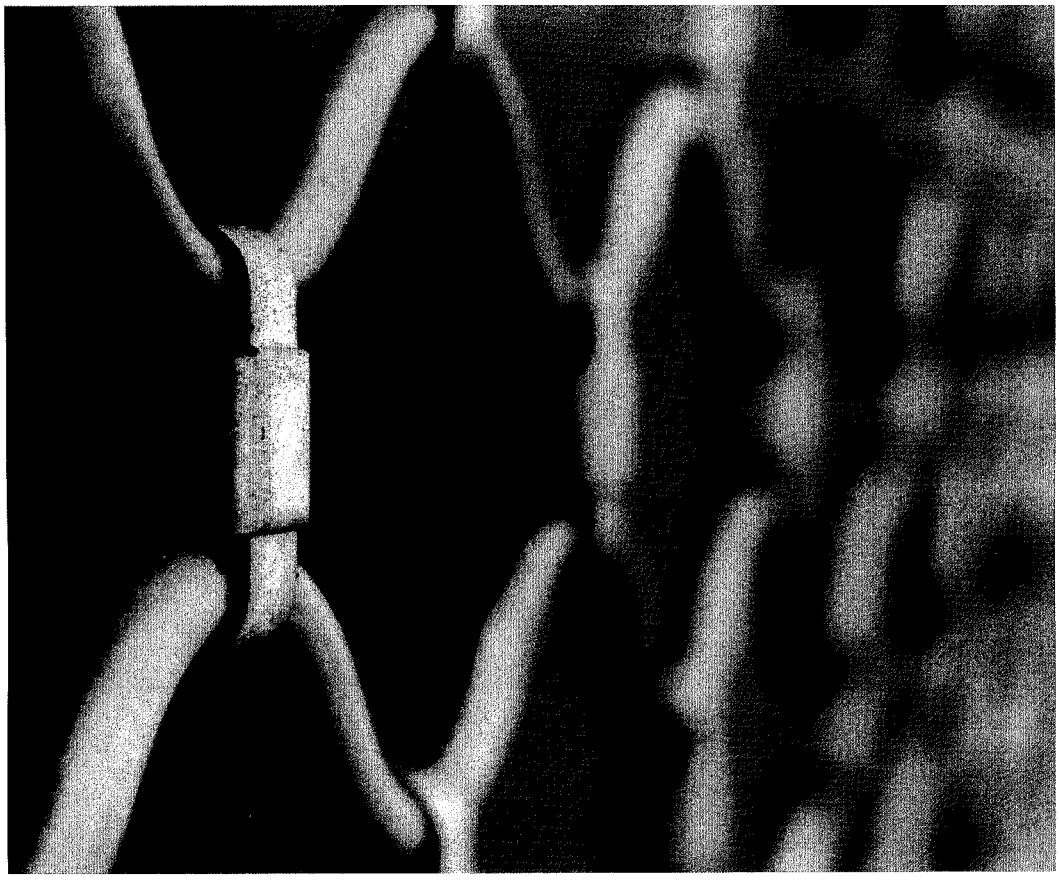
That 'front line' in larger organisations may be the only protection barrier in smaller business. That is precisely why the UTM appliance will make an increasingly valuable contribution as a comprehensive security solution in a single box. "The user actually can't screw it up," was the worldly wise observation by more than one of our interviewees. ■

Publication: Computerscope
Date: Thursday, May 18, 2006
Page: 39
Extract: 5 of 6
Circulation: 9.681
Author:
Headline: One for all

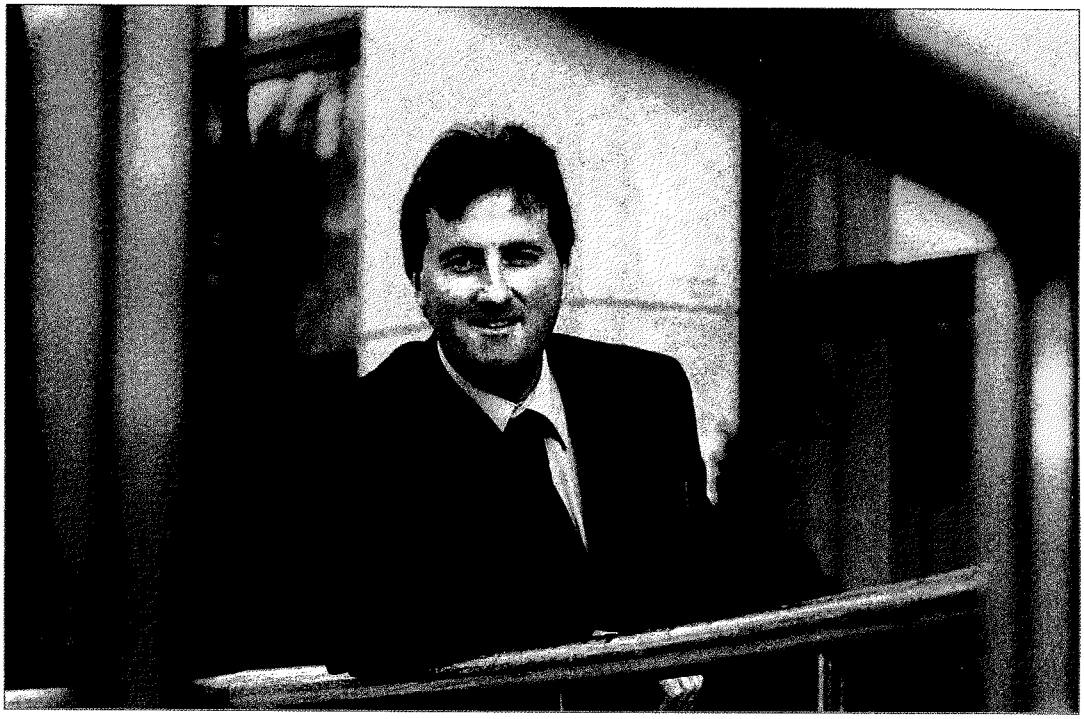
'One of the great strengths of the UTM approach is that security updating is automatic and remote'

There is a modest amount of initial user configuration required'

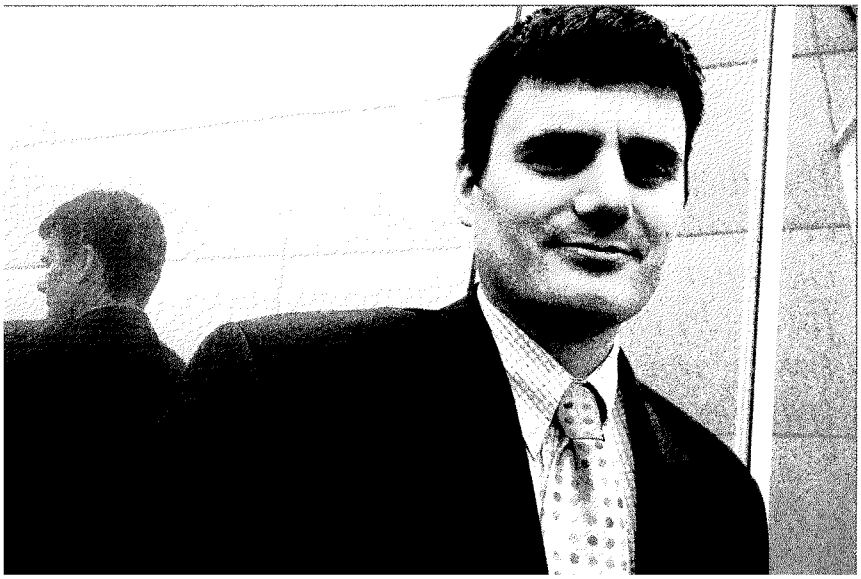
'The good thing about UTM is that is simplifies security so that the protection of the applications in the box will actually be fully implemented'



Publication: Computerscope
Date: Thursday, May 18, 2006
Page: 39
Extract: 6 of 6
Circulation: 9.681
Author:
Headline: One for all



There is the question of the multimodal ways in which we communicate with our networks and the Internet, Sean O'Connell, CA



There is certainly a trend towards ever-smarter boxes, Ray O'Connor, 3Com