



PERIMETER

29

All Things to All Men?

Rik Turner examines the growth of the unified threat management appliance, asking whether it is all things to all men, or jack of all trades and master of none.

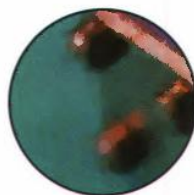
The term unified threat management (UTM) was coined by analyst firm IDC in 2004 to describe a trend in the information security market whereby an increasing number of vendors were launching gateway appliances, onto which multiple edge security functions were bundled.

The IDC report, published in September 2004, studied the market in the previous year and made forecasts for the next four. It predicted that the UTM appliance market would enjoy a compound annual growth rate of 17% through 2008, when it would represent 60% of a global security systems market of \$3.45bn.

THE HYPE-CYCLE BEGINS

IDC followed that with another UTM report the following year, complete with another four-year forecast (to 2009), predicting an even more dramatic CAGR. Each report's vendor ranking for the previous year's UTM market became hot property for marketing departments, with different developers claiming market leadership globally, in Western Europe, in the high-end, and so on. Indeed, given sufficiently narrow categories and sub-groups, everyone could be a market leader somewhere.

UTM is less of a revolutionary development and more of an evolutionary one. Prior to IDC's creation of the



category, vendors of one or other of the multiple edge security functions like anti-virus (AV), anti-spam (AS), anti-spyware, intrusion detection and/or prevention systems (IDS/IPS) or filtering, were gathering up other features into software bundles, whether through partnership or acquisition.

Equally, there had been a marked trend towards offering single-edge security functions on appliances, usually comprising commodity hardware and a hardened open source operating system

such as Linux or BSD. As such, it was only a question of time before someone put the two together to create multi-function security appliances, and when they did, IDC was there to name the child.

Most UTM appliances in those early days were aimed at the SME/SMB market, the logic being that customers would be attracted by their promise of 'drop-in' ease of deployment, reduced ongoing running costs and the all-in-one security fix.

Vendors from the software-only, single-function end of the information security market might argue that multiple features in one box were not necessarily the best products in each category, and that each separate security function would still require separate management, but the UTM device clearly captured the imagination of a segment of the market, and they are evidently here for the long term.

Companies making the running in UTM back then were not household names in information security, however. They tended to be start-ups created to take advantage of an inflection point in the market, delivering multiple security functions in one box to SMBs, who previously might not have gone much beyond AV licences on desktops.

In that first year IDC made Fortinet the market leader, although SonicWALL, arguably even more SMB-focused than Fortinet, made it in one sub-sector.



Another challenger in the space from the outset, and again very much in the SMB market, was WatchGuard.

Some of the more established names in the security market soon joined the fray. ISS, market leader in IDS/IPS as software sold into enterprise, was one of the first big names to get into UTM. Developing an appliance strategy since early 2003 with its Proventia range of boxes, by October that year it was announcing the first multi-function device in the range, the Proventia M50. It followed up in mid-2004 with the Proventia M10, a truly SMB device.

ENTER THE BIG FISH

The Big Three AV heavyweights, Symantec, McAfee and Trend Micro, all entered the fray, the Japanese ISV being the last to market with a device, launching its InterScan Gateway Security Appliance only last year. By then Symantec was making an exit from the market, at least in terms of developing its own hardware.

However, what was widely interpreted as a full-scale withdrawal when announced in July turned out to be something different two months later. The AV behemoth announced a broad partnership with router and firewall vendor Juniper, covering both network access control (NAC) technology and UTM devices.

McAfee faced problems in UTM in the shape of a lawsuit brought last year by small US information security developer Deep Nines, claiming infringement of a patent it holds on technology for combining a firewall and signature-based intrusion detection and prevention technology into a single appliance.

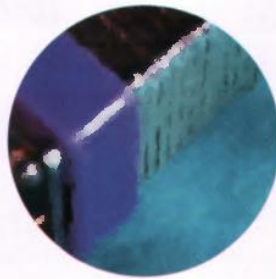
The market leader in firewalls, Check Point, last year launched a bundle of security functions, entirely in software, calling it VPN-1 UTM. This year it launched an appliance version of the same technology. Nick Lowe, managing director for Check Point Northern Europe, evokes the roadmap for the company's offerings in the space.

"Going forward, UTM solutions need to move beyond simply consolidating popular security functions at a single site, to consolidating security management across the entire infrastructure. This includes deploying new security protections, updating existing security functions and providing useful monitoring and reporting."

Secure Computing, meanwhile, offers both a UTM version of its Sidewinder firewall at the higher end of the market



In 2004, IDC predicted that the UTM appliance market would enjoy a CAGR of 17% through to 2008, when it would represent 60% of the global security systems market.



and a low-end UTM appliance that it got through its acquisition last year of rival vendor CyberGuard.

Second-tier AV vendors have also entered the UTM market of late. Spanish AV vendor Panda Software launched its offering in 2006, while Germany's Astaro has come to market with one this year.

Walter Schumann, Astaro's VP of sales and marketing for EMEA, says that "originally, IDC defined UTM security appliances as products that included network firewall capabilities, network intrusion detection and prevention, and gateway anti-virus functionality. However, UTM vendors have begun integrating many more applications."

ZyXel and D-Link, both companies from SoHo networking and security with

ambitions in SMB – where they hope to win share through price competition – have also launched UTM devices.

It is not only information security specialists that have been attracted to the emerging market. Networking vendors, led by Cisco, have been encroaching on the security market throughout this decade, and indeed, this was one of the drivers for hitherto software-only companies such as ISS to adopt appliance strategies in the first place. It was only natural, therefore that they too should succumb to the attractions of UTM: Cisco now offers its Adaptive Security Appliance (ASA), while Juniper has its Secure Service Gateway (SSG).

3Com, an erstwhile heavy hitter in networking but now a shadow of its former self, seeks a return to the top table, partly through security, based primarily on the TippingPoint IPS technology it acquired in 2004. The following year it introduced the TippingPoint X505, a UTM box that, in addition to IPS, ships with a stateful firewall, web filtering, an IPsec VPN and traffic shaping based on policy.

Nortel has said less about UTM devices than its competitors, but its partnership with Check Point suggests that whatever it does in the space will come from that collaboration. Check Point provides the firewall inspection engine for Nortel's Switched Firewall offering, and Kiran Ghodgaonkar, product manager for Switched Firewall, was quoted earlier this year as saying that, "UTM is the direction the industry is going in... [but] the problem comes back to performance. Turning on all of these features is very processor-intensive. Coming up with an architecture that can handle all that is where the market needs to head."

HIGH-END UTM

One company has taken this high-end approach to UTM from the outset, namely Crossbeam. Although in the security market, what it actually brought to the party was networking expertise, leaving security functionality to partners.

Crossbeam designed a high-end chassis with a switched backplane into which partners in the different segments of infosec like Check Point (for firewalls), Sourcefire and ISS (IDS/IPS), Websense (filtering), Trend (AV) and Forum (XML security) can deploy their products. In other words, it provides optimised real estate for a multi-tenant security appliance for service providers and very large companies.



32 PERIMETER

Key players

Astaro

This German security vendor offers its Astaro Security Gateway both a software and as an appliance, providing email, web and network security in a single box. Seeking differentiation from the pack, last year it teamed up with fellow German company Utimaco to use its email encryption, digital signature and verification technology on its appliances, claiming to be the first vendor to offer such services on a UTM device.

Check Point Software

The US/Israeli firewall vendor – with joint HQs in Ramat-Gan, Israel and Redwood City, California – was a late entrant into the UTM market, debuting with a software bundle called VPN-1 UTM last year, and only finally producing a hardware version, called UTM-1, in February. This is recognition that, if it is to make inroads into the small to medium business market, having its own hardware is essential. While Check Point is late to the party, do not underestimate the power of its channel and partners to help it make up for lost time.

Crossbeam Systems

Crossbeam started at the high end and is working its way downmarket, with its strategy being to provide the optimised infrastructure, in the form of a chassis and backplane, for multiple infosec software vendors to deploy their technology as blades. Partners include Check Point (firewalls), Sourcefire and ISS (IDS/IPS), Trend and Panda (AV), Forum (XML security) and Websense

(URL and peer-to-peer filtering). The company is currently in the process of adding intellectual property leakage protection with technology from Websense's newly acquired PortAuthority business.

Finjan

Finjan offers a range of UTM devices called the VitalSecurity Web Appliance family, for markets from SMB to large enterprise. While they ship with all the standard features such as AV, anti-spyware, URL filtering, SSL inspection and a behaviour-based inspection engine for finding and blocking unknown threats, a differentiator on the products is Finjan's Vulnerability Anti-dote technology to perform virtual patching for what it calls 'zero-hour' protection against known vulnerabilities.

Fortinet

Many observers would argue that Fortinet is the very epitome of a UTM vendor with its FortiGate product line, shipping with firewall/VPN, IPS, AV, web filtering and traffic shaping and targeting SoHo and SMB customers. There are some important departures from the norm, however. First, Fortinet does not use commodity hardware or a hardened open source OS, but rather runs its FortiOS operating system on its proprietary FortiASIC processors. Second, Fortinet has outgrown the low-end market, buying first the intellectual property, then the assets and customer base of enterprise and carrier UTM vendor CoSine. Not surprisingly, as a result of this expanded remit the company

has begun evangelising about the need for 'clean pipes': the notion that edge security can and should be delivered in the service provider cloud, with malware being taken out before it ever reaches the enterprise.

IBM/Internet Security Systems

Last August IBM spent \$1.3bn to acquire ISS, a security developer whose original claim to fame was to have been one of the pioneers in the development of intrusion detection software (IDS) in the nineties. By the early part of this decade ISS was pursuing an appliance model to take it downmarket from the traditional enterprise customer base for its software-only offering. Initially its Proventia appliance range was single-purpose around its IDS and, by then, IPS technology. However, in 2003 it began shipping the Proventia M series of multi-function UTM boxes.

Panda Software

Spanish security software developer Panda Software launched the unified threat management device in August last year, calling it the GateDefender Integra. The Integra box combines the functionality of Panda's existing content security offering, the GateDefender Performa (AV, anti-spam, mail and Web filtering, including HTTP and FTP) with a firewall and VPN capability. The anti-spam is provided by Panda's partner MailShell, while the VPN technology is OpenVPN and an IDS/IPS capability is provided by Snort. The company also recently launched Malware

Radar, an automated malware audit service.

SonicWALL

Another of the early entrants into this market, SonicWALL is in some ways even more UTM, in that it does continue to target SMBs first and foremost, despite now having enterprise and MSP products in its portfolio, and also because it leverages commodity hardware and open source software for its SonicWALL TZ and PRO Series of appliances. If anything, the big news from this company has been its diversification into other technologies suitable for the SMB space and delivery on appliances, namely storage (back-up and restore) and remote access, as a result of the acquisitions of Lasso Logic and enKoo at the end of 2005.

Symantec/Juniper Networks

Juniper Networks spent \$4bn in 2004 to acquire NetScreen Technologies, a company that had stolen a march on market leader Check Point by delivering firewalls as appliances. That business and its ScreenOS now form the core of Juniper's UTM offering, the Secure Services Gateway (SSG). Meanwhile Symantec had been developing its own appliances since the early part of this decade, but last year announced it was ceasing hardware development and teaming with Juniper for work in both the UTM and network access control (NAC) market, in what looks like a face-off with Cisco.