

# Security:

## It's getting hot in here!

**Recent world events and a year of harmful virus attacks have placed security issues at the forefront of many people's minds and smart channel players are cashing in on the trend**

**By Sholto Macpherson**

It's a simple fact that most companies will try to get away with the bare minimum of protection. After all there is no such thing as total protection; it will always come down to some compromise revolving around the number of dollars in the IT budget.

But the acceptable minimum requirement is growing. Firewalls are a product that make perfect sense to any company that can easily understand the concept of perimeter defence.

The firewall has evolved into a more complicated beast, with integrated, subscription-based services such as content filtering and VPN

bringing greater protection and opening the door to recurring revenues.

The most wanted feature is antivirus protection, now at the forefront of the security consciousness after a shocking year of blended threats. More medium level and above viruses were detected in the first quarter of 2004 than in the whole of 2003, according to Network Associates.

The sustained assault has elevated antivirus protection to the top of the pyramid and is now commonly featured within the firewall itself and not just on individual PCs.

These extra features are turning the firewall from a single-sale appliance into a handy earner. Updates require

regular contact with the customer and an ongoing consulting role; in a security environment that is constantly changing, a company's protection must take account of new threats and the company's own growth.

A basic updating service requires little more than a customer service centre and an engineer to carry out the updates, which are largely automated. 'That's very easy money,' says LAN 1's managing director, Daniel Lee.

He recommends that a good reseller should have at least 100 sites to provide a solid income stream based on the annuity of renewed licences.

The more features the better the margin, and the



**Fortinet's Sandilands: Vendors have switched onto the holistic security game plan, but resellers have been slower**

SME market has been willing to pay. But the downside is added complexity; knowing how to integrate each appliance into a custom network is an issue for resellers, says Lee.

The pace of technological improvements combined with the growing demands of the market threaten to outstrip the knowledge base of resellers. Without well-briefed staff running installations, protection of each layer using the latest products is hit and miss. 'Training is going to be the key,' says Lee.

Another trend is the narrowing of security products on the market: competing products in each new range are selling the same sets of features. The commodification of security appliances is not happening as quickly as other areas of IT – margins are holding at around 15 percent, says Lee – but the trend emphasises

that a reseller is safer in consultation and design.

One newcomer to the firewall scene that does stand out is Watchguard's Firebox X. The range of multi-function boxes differs only in the number of features, each of which can be unlocked by a licence key.

Customers can buy a low-specification box and upgrade as needed without the disruption to business caused by a forklift upgrade, says Watchguard's regional director for Australia and New Zealand, Sven Radavics.

The only requirement, a 40-second reboot, is much less painful than the average two- or three-year technology refresh.

Features include VPN, content filtering and URL filtering, with antivirus in the pipeline.

The security on-demand model echoes IBM's own

approach to utility computing and could give Watchguard the edge in the highly competitive firewall space.

One of the big advantages to resellers is that an upgradeable firewall ties in a customer for several years rather than losing out to a competitor that can offer better features or a lower price the next time an upgrade is needed.

Another plus is that the single renewal for each box has been replaced with individually renewed services, says Radavics.

For the reseller it means taking high margins on a full firewall upgrade with minimal work; for the end user, a better deal from a TCO perspective.

Although the Firebox X range has only been out since the beginning of February the results have been interesting. John Labza, managing director of Firewall Systems, a distributor specialising in security, says that companies purchasing a firewall used to buy what they could afford, not what they needed.

Now customers are going for lower specification models of the Firebox X range knowing that they can upgrade only when it is absolutely necessary.

This initial cost saving often turns out to be more expensive in the long run. Buying a low-end system and then an upgrade in 12 months is less cost-effective than spending up on a bigger system from the start.

However, this is all good news for resellers, and good news too for customers who need to stagger their IT purchasing over a more affordable time frame.

#### **Keep in control**

Management is the next issue vendors are racing to address. In the face of blended threats, the time it takes to update defences once a new threat is

discovered is crucial. This has put pressure on vendors who play the best-of-breed game and handed some advantage to companies selling all-in-one appliances.

'Integration' is a buzzword that closely follows any mention of management in the business world, and as any reseller in any field knows, integrating products from several vendors is never as easy as promised.

But many vendors are adding management to their portfolios in a bid to stay relevant.

'Anyone who is serious about playing in this area has to try and tackle the

is moving into similar territory.

Global vice-president Jerry Ungerman was in Australia recently talking to partners and customers about two products, one addressing the defence of internal networks and the other web portals and content delivery.

Ungerman says that, apart from updates against application-level attacks, the network layer 'is pretty well protected for enterprises'.

Although 70 percent of the company's revenues come from VPN sales, Ungerman admits that some old partners still view Checkpoint as a

'Anyone serious about playing in this area has to try and tackle the management issue'

management issue,' says Fortinet's Peter Sandilands. While vendors may have already switched onto the holistic security game plan, Sandilands adds that resellers and customers have been slower to take the next step.

Instead, firewalls are viewed as a perimeter device, antivirus as a desktop problem; failing to address the two as key parts of a united defence plan leaves companies in a weaker position, says Sandilands.

Fortinet's answer is the all-in-one appliance, a trend that Sandilands believes is unstoppable. And Fortinet is pushing hard the compatibility of its management software with its own hardware over a security package that tries to bring together products from multiple vendors.

Checkpoint Software, a vendor that built its reputation on the quality of its firewalls,

firewall specialist 'that never really graduated into VPNs'.

Now the challenge is in delivering products that move beyond the perimeter, and in addition to the web portal and internal network products already mentioned, Checkpoint has introduced its own answer to centralised security management based on the Zonelabs product the vendor acquired late last year.

Several distributors, including Dovetail Distribution's general manager, Max Fredericks and LAN 1's Lee, confirm the popularity of the all-in-one appliance. Customers who already own some level of protection are implementing a second, all-in-one appliance for the added features and doubling up on protection, says Fredericks.

The security specialist says the all-purpose Fortinet products have been selling well



**Watchguard's Radavics: Customers can buy a low-spec box without the disruption caused by a forklift upgrade**

particularly because they bring antivirus forward to the gateway. Fredericks says a layered approach to security, with antivirus protection at the perimeter and on the desktop, is essential for providing complete protection.

Although many resellers are passing up the opportunity to secure the customer at both ends, Fredericks believes the shift in strategy from perimeter to individual employees is well under way.

In what must be a relief for Checkpoint, the only other strong-selling product that Fredericks mentions is the central management platform developed by Zonelabs. Fredericks echoes vendors' concerns that resellers are slow on the take-up in management despite the number of products available.

Another area that is showing significant activity is remote management, which hands the reseller a strong connection with customers as well as potentially years of recurring revenue.

Network Associates is promoting a managed security service based on McAfee ASAP that delivers web-based reports to the reseller on virus

activity and security status for each machine. Designed for the smaller reseller, the service targets SMEs that are generally uninterested in monitoring their own security and were willing to outsource all their IT requirements.

While security is the obvious focus, senior marketing manager Alan Bell says the service opens a window into more general management issues. Resellers can monitor the performance of servers and desktops and suggest software and hardware upgrades based on these reports.

Resellers already using the service have maintained visibility with customers by mailing a full-colour, graphical report with the monthly invoice – a necessary step to remind customers what they are paying for.

#### **Processors don't sell, processors do**

With so many appliances, applications and policies in the security sphere, it is easy to become focused on the technology. It is not enough to know exactly what features a firewall has or even how to plug it into an existing network.

CEOs don't need to know these details or whether one appliance is better than another – they need a business case that explains why their company can't do without it.

'You can't just go into a company and sell a firewall,' says Firewall Systems' Labza. 'You have to do a business level approach that a CEO will understand.'

In security that case is business continuity. This was the theme of Security Café 2004, an event organised by Firewall Systems where resellers and end users listened to vendors and consultants give advice on how to sell security.

Risk or threat analysis is a legitimate concern for every

company and provides the best opportunity to gain an audience with senior management, says Labza.

Risk management policies constructed around the threats to business operations call on a much wider portfolio than security. The issue becomes less about stopping hackers and more about business uptime, an area that includes related services such as redundant internet connections, backup links and disaster recovery.

Redefining security more generally can lead to other opportunities left unexplored. While physical security is unfamiliar ground for most resellers, cracks are opening up in surveillance, traditionally the area of CCTV specialists such as Honeywell.

CCTV is still the dominant method for recording surveillance but the growth of IP-based monitoring is slowly catching on.

IP cameras can now be had for less than \$200 and LAN 1's Lee hopes resellers will start to look across the board to digital storage rather than video tape.

Biometrics, another player in physical security, still has not materialised in any significant way. Lee considers it 'a nice topic to talk about, but it is not widely demanded'.

However, new markets also mean new competition. Selling risk assessment and management at the higher end takes resellers into the same territory as accountancy firms and, potentially, legal liability.

Some vendors claim that there is little to be worried about – one remarked that because no reseller had recently been sued, it was unlikely to ever happen.

Nevertheless, it pays to read the fine print or – more importantly – write it yourself. Network Associates includes terms and conditions



**Brennan IT's Stevens: Regardless of the brand or model of firewall, it is very difficult to examine every single packet for its content**

which exonerate the company and reseller from responsibility in the event of a security breach.

But the perception of responsibility inevitably rises with the price of a contract and some companies are keen to ensure that professional advice is backed by legal accountability.

Labza recounts the experience of an independent consultant attending Security Café 2004 who was approached by a large company looking for a risk assessment and policy.

When the consultant asked why the company's own accounting department did not carry out an internal audit the company man replied: 'Because we can't sue them'.

#### *Are you insured?*

Labza is not alone in viewing security as an ongoing role for a reseller rather than a drop-and-go purchase.

SonicWALL's channel marketing director Dave Crilley looks at security as a productivity insurance policy and that monthly rates in return for business up-time are easily justifiable to any customer.

In this secure relationship the cost of new equipment can be billed over several months, adds Crilley.

'The managed security service provider is the hottest thing going right now in terms of driving high-margin, incremental revenues to resellers' business,' says Crilley.

Symantec's Donovan is one of the few vendors who shows some restraint in advocating the rush to becoming a managed service provider. 'There's a big jump between supplying software and remotely managing or monitoring security,' he says.

While many Symantec resellers are MSPs and the vendor is willing to provide free certification and training for new recruits, providing remotely managed security services requires significant investment in equipment and skill sets.

'It's a fairly rarefied atmosphere,' says Donovan.

The market for outsourced security is growing at 100 percent year on year – admittedly off a small base, notes Donovan – but he believes the current number of MSPs adequately cover the market.

This is partly due to the shift in culture required by SMEs to let go of IT staff and place their faith in a reseller. 'It's a big step for a company to take,' says Donovan.

There are obvious advantages, but one interesting fact is that the risk of a targeted



attack drops the longer the tenure with an MSP, says Donovan. He attributes this to the familiarity of security policies, the constant hunting for weaknesses and a reputation within the hacker community that the company is a tough target.

Not every customer requires a full risk assessment and management strategy spanning mobile phones to firewalls. There are plenty of SMEs that would benefit from simple pointers on security policy and compliance.

Any reseller can fill the role of adviser and offer a range of zero-cost measures that minimise the opportunities for a security breach. Disengaging default firewall settings, turning off file-sharing, regulating network usage – these basic steps can go a long way towards improving protection, says Donovan.

Wireless remains a weak point in network security. Rogue access points are still a problem as the free-roaming

individuality of wireless sometimes encourages end users to take matters into their own hands when it comes to finding a way back onto the company network.

VPNs have become an accepted method for controlling access, but wireless hotspots in CBDs and travel lounges can become hot zones for Trojans and worms. Firewalls on notebooks are not yet a standard feature and even less likely on other IT devices.

Notebooks are only one part of the equation these days; PDAs have become more common in the corporate and consumer world, as have high-end mobile phones capable of carrying data.

Symantec has been pushing their own remote management package, Client Security 2.0, to protect a network from remote and networked clients. The centrally managed application updates every machine on its network with a single update mechanism that combines virus definitions, firewall

rules and intrusion detection signatures.

In a case of tough love, Client Security protects the corporate network first by denying access to clients that don't comply with network policies.

'It enforces corporate policy regardless of where the user is,' says Donovan. The management console also lets network managers check whether clients are protected and whether they are VPN compliant.

LAN 1's Lee believes that mobile devices have made VPNs a must-have item for most SMEs. The distributor also has a product approved for GPRS, however this has been slow to move off the shelves.

#### The road ahead

Despite tumbling CPU prices and consistent power increases, the sheer volume of data flowing over corporate networks can often overcome the sturdiest of firewalls.

Better filtering is the current flashpoint in security as the majority of attacks come through port 80 (HTTP) or port 25 (email). Some lower-grade firewalls avoid the issue altogether and leave these ports wide open.

Regardless of the brand or model of firewall, it is very difficult to examine every single packet for its content and decide whether it is harmful, says Brennan IT's managing director David Stevens.

Stevens sees insufficient processing power as a bugbear of content filtering boxes which just 'don't have the muscle' to operate intrusion-detection circuits transparently. On a 100Mb connection 'we're basically slowing down the traffic', he says.

Labza believes the answer is the application-specific firewall such as Borderware Technologies' MXtreme appliance. Sitting in parallel, it deals with all email travelling

through port 25, which relieves the pressure on the main firewall.

Email messaging is essential to the operation of most companies and a dedicated firewall that can deal with spam and infected attachments is an easy sell for any customer that receives orders or payments by email, or hospitals which email patient records.

Spim - spam for instant messaging - is also destined to become a bigger issue as instant messaging makes the transition from social to corporate tool. Dedicated products are also emerging in this space.

Another technology slowly making its way to the fore is IP telephony, which Labza says will also need better protection than current measures. The digitisation of telecommunications will reopen the possibilities of making free phone calls at company expense or hacking into the CEO's voicemail, says Labza.

Unsurprisingly, vendors in the VOIP space are playing down the likelihood of these scenarios. Cisco's consulting systems engineer, Brad Engstrom, says the susceptibility of digital networks to interference or tapping is no greater than the current analogue systems.

Cisco responded to fears of phone tapping by introducing encryption to its VOIP phone range, although Engstrom still maintains that concerns over phone-tapping are exaggerated. Conventional phones are easily tapped if a hacker has access to the building, says Engstrom.

And hacking exchanges still exist. It is still possible to dial into PABXes, forward calls to international numbers and hack into voicemail accounts. There is no reason to believe the situation will get any worse under VOIP as the same voicemail products run



**Firewall Systems'  
Labza: You can't just go  
in and sell - you need  
a business approach  
CEOs can understand**

in both VOIP and PABX environments, says Engstrom.

Taking a different tack on the fight behind the firewall, Cisco is just releasing its Security Agent application which looks for bad behaviour on individual machines. Instead of trying to determine whether attachments are dangerous, CSA watches whether a PC starts behaving in a way that is different from its normal operation.

A company can set CSA to ask for confirmation for activities like downloading software or launching an application. If this is what the user is trying to do, CSA steps back and lets the computer proceed as normal. If it is an unexpected activity, it will block it.

Engstrom says that CSA needs to be carefully set up for every company, opening up a strong consultancy role for the reseller. Cisco supplies a tool that constructs profiles of PC behaviour to aid in determining an appropriate rule set and applications for each machine.

CSA may seem like protection with limited use, but its value is in defending against the zero-day attack where a hacker writes a virus to exploit a vulnerability previously unknown to security vendors, says Engstrom. □