

In a world of multiple threats, resellers can help companies secure the fort by offering a holistic security approach. JENNIFER O'BRIEN reports.

Today's trend towards consolidated security moves the industry beyond a band-aid appliance approach to embedding security into the entire enterprise network. For resellers, having more security solutions from fewer vendors means less confusion and better business.

Indeed, the move towards the integrated path — where centralised standards-based security is becoming the norm — started in response to last year's Year of the Worm, managing director of Enterasys, Gary Mitchell, said.

The threat had morphed from the network's boundaries to the application layer with internal users often providing the springboard, Check Point Software's regional director A/NZ, Scott Ferguson.

According to IDC, 80 per cent of all security products would be delivered

as appliances within other hardware devices within the next five years — a change that would make security initiatives easier for enterprises.

Security challenges were becoming more complex as the perimeter becomes fluid, IDC said. Given the reliance on mobile and wireless technology (PDAs, mobile phones, laptops and WLAN), along with the bulging reams of data, companies needed to protect enterprise data on all fronts.

The appliance approach will help ward off new cyberspace nasties that are popping up including the convergence of viruses and spam. The technology will also help deal with the rapidly shrinking discovery of a vulnerability to an exploit.

Security expert at Network Associates, Alan Bell, said the increasingly rapid rate at which the worm and virus writers were exposing vulnerabilities would be the biggest challenge for the IT manager in 2004.

► to page 36

March 31, 2004

◀ from page 33

The patch management approach, he said, would be an ongoing and increasingly difficult challenge for the IT and security staff.

And since security is a critical enabler of business continuity and linked to the survivability of an organisation, companies need to consider their technology moves carefully, according to IDC.

Gartner suggests malicious-code attacks at the application, network and data levels will drive new security infrastructure approaches in 2004 including deep packet inspection, intrusion prevention and personal firewalls deployed across the enterprise.

Companies need to pump up their security efforts in five areas: security policies and architecture; security infrastructure; security administration; business continuity management; and critical infrastructure protection.

IDC suggests taking a look at three key areas: policies, people and processes.

Organisations needed to address privacy, security and business continuity when looking at policies, IDC Asia/Pacific's research manager for security/infrastructure software, Natasha David, said.

When addressing the people portion, companies needed to ensure the C-level executives were driving the security strategy, David said.

"Currently 60 per cent of enterprises worldwide are driving their security policies from the IT or IS manager level, with only 17 per cent being driven by business managers," she said. "This obvious liability is becoming a major issue and company directors need to take the lead."

With processes, organisations need to address the issues of integrating physical and network security.

"From front door access to online exchanges with customers, potential risks must be identified and processes determined early," David said.

Combat mode

Given that the security landscape has changed dramatically over the last few years, blended threats require industry collaboration, said Randy Pond, Cisco Systems' vice-president of operations, processes and systems.

As such, Cisco is on a push to generate demand for its self-defending

network technology. As part of the global strategy, the latest extensions will help identify threats, react based on risk level, isolate infected endpoints and reconfigure the network resources in response to an attack.

Through a collaboration with Network Associates, Symantec and Trend Micro, the self-defending network initiative helps customers identify, prevent and adapt to security threats.

"Traditionally Cisco hasn't been connected with security," Pond said. "But we want to make sure the Cisco brand is recognised," he said. "Point solutions don't protect from all threats, so we need a broad approach embedded in the client's network."

On Australian shores, channel man Kip Cole said Cisco sees strong growth in security — in particular making sure the entire network is secure. "Ensuring security is a network service to be embedded throughout the infrastructure."

Most enterprises are at risk because of rogue access points, Pond said. As such, collaboration amongst industry players is needed. "You need ubiquitous security in the network to make it all work. And all of us have to play a role in this."

As part of the threat defence system line-up, Cisco has rolled out an IP Source Tracker (a Cisco IOS software-based security product), and new firewall support.

Under the connectivity and security management banner of products, Cisco has unveiled the 7301 router, the Security Device Manager Version 1.1, and the VPN 3020 Concentrator.

And Cisco isn't alone in the push towards embedding security into the entire network. Since the perimeter is no longer the firewall, players are rolling out an holistic approach.

"Vendors are pumping out hardware that is better equipped to deal with a range or even a blend of security threats," NetGear Asia-Pacific's managing director, Ian McLean, said.

Products on the market supported an increasing host of security features, ranging from firewalls through to point-to-point tunnelling and Layer 2 tunnel protocol for VPN pass-through support, he said.

"The way people think about security has to change," Fortinet's regional manager, A/NZ, Peter Sandilands, said. "We tend to think of it at the perimeter-based

level, but in reality it is pervasive across the entire network."

He said the company was taking its complete content protection message to the channel, and recently completed a round of certification training with resellers in Sydney and Wellington.

The company wants to get resellers jazzed up about the hardware, which lets users analyse information flow across all network levels.

"A virus — a large one — may span multiple packets," Sandilands said. "So we need to look at the contents of large numbers of packets."

"We get up close and see the conversations occurring. It takes information out of a number of packets flowing between devices. Today, devices built around firewall only look at individual packets."

Anticipate risks

Whereas Cisco might be pushing a similar message, Sandilands said the approach was different.

"Cisco is pushing its capabilities into the existing platform through switches and routers, but we can build a special piece of hardware," he said.

Enterasys, for its part, aimed to help companies integrate security into the entire network infrastructure rather than adding it as an afterthought, Mitchell said.

"The idea is to anticipate risks before they occur," he said. "We believe the network needs to be able to react very quickly to threats unknown."

Dubbed Enterasys Secure Networks and available to resellers this month, the technology provides total network visibility; identity and context intelligence; distributed policy enforcement; centralised, granular control; system-level management; and dynamic response and protection.

"From a network perspective, we're moving beyond performance, speeds and feeds and now understand the network must play an active role — it needs to become more intelligent and take a more proactive role in security defence," Mitchell said.

Network Associate's prevention strategy, meanwhile, which was now launching into the channel, involved an intrusion protection system (IPS) that combined detection and resolution to close the vulnerability before the damage was done, Bell said.

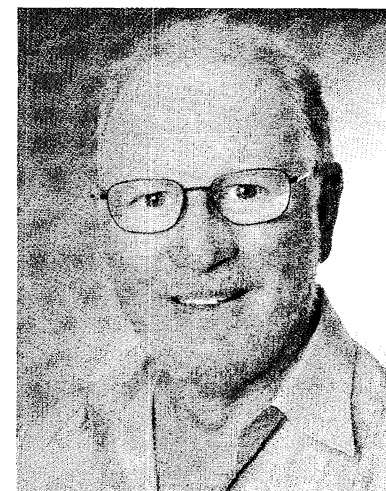
The latest technology is launched in connection with the ASAP Partner



Network Associates' Alan Bell: IT managers face major challenge from worm and virus writers



NCR's John Burgess: Services are an essential part of the prevention plan



Fortinet's Peter Sandilands: "The way people think about security has to change"

◀ from page 34

Monitoring Service, which lets a reseller provide remote virus monitoring of an SMB's network.

Product marketing manager for Trend Micro, Clive Wainstein, said no security solution had stopped or contained network viruses, which totalled \$US2.15 billion in damages in 2003.

"No single technology can adequately protect against the complex threats we are beginning to see," he said.

As such, the rollout of the Network VirusWall would help companies deal with the patch management conundrum and the problem of reinfection, Wainstein said.

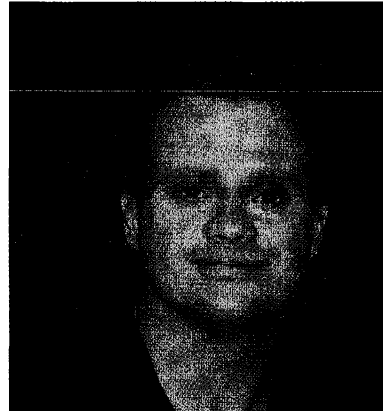
"It's almost impossible to keep up with vulnerabilities and patching," he said. "And there is no knowledge of which virus is likely to exploit vulnerabilities."

The company was pitching its enterprise protection strategy, which Wainstein said was designed to deliver protection at both the application and network layers to proactively manage the outbreak lifecycle from vulnerability prevention to malicious code prevention and elimination.

The company wants to take the message to its 150 resellers throughout Australia.

"The idea is to help an enterprise stop, quarantine network virus and enforce security policy," Wainstein said.

Benefits include a reduced security



Trend Micro's Clive Wainstein: Pitching a policy that delivers protection at both application and network layers

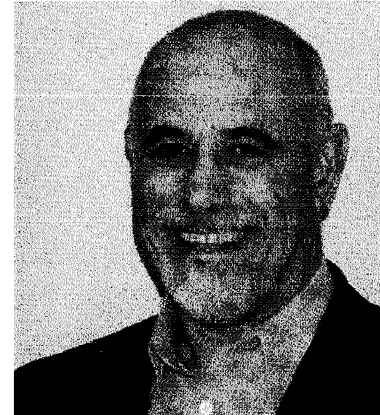
risk, network downtime and the outbreak management burden.

"Network worms are almost on steroids, getting developed to penetrate deeper, faster and in multiple different methods," he said. "And what better way to get the message across than to piggyback spam with a network worm. It's starting to become a new world."

The technology, which is aimed at both enterprise and the SMB space, scans the network in real-time.

"The network administrator knows what's going on, and can stem the flow of the virus and identify sources of infection," Wainstein said.

What's needed, Gartner suggests, is a scan, block and quarantine approach to survive worm attacks and guard against blended threats from spreading through internal networks.



Secure Computing's Eric Krieger: "Channel/vendor relations becomes a nightmare when spread across so many players"

Change your security infrastructure to refuse connections from unsafe PCs and mobile devices, Gartner said.

Secure Computing, meanwhile, is on a push to generate demand amongst resellers for its suite of multi-function appliances that deliver a gaggle of security applications in a single device including application firewall, VPN, anti-spam, anti-virus and management tools.

Secure Computing's regional manager A/NZ, Eric Krieger, said the launch was in response to strong channel demand for consolidated security solutions.

"Channel/vendor relations become a nightmare when spread across so many players," he said.

Meanwhile, enterprise customers — particularly government, banking, manufacturing and telecommunications — are also looking for fewer vendors.

"There's been a strong pent up demand for consolidated security solutions," Krieger said.

But in addition to ensuring good IT security infrastructure and systems, NCR's professional services manager, John-Paul Burgess, said services were also an essential part of the prevention plan.

He said companies forgot that regular reviews and penetration testing, especially of newly-developed applications and newly-implemented systems, were of critical importance to highlight areas of weakness.

MS gets busy with spam

Microsoft rolled out two security initiatives last month that aim to improve email authentication and enterprise boundary protection to fight spam.

The Co-ordinated Spam Reduction Initiative (CSRI) and Caller ID for email will let enterprises identify message senders and determine their legitimacy.

The other initiative, the Microsoft Exchange Edge Services, will enhance Simple Mail Transfer Protocol (SMTP) to guard against spam and viruses, making mail delivery more efficient.

While Gartner suggests the initiative will have limited success — in part because there's a lack of credibility in the security of Microsoft products — it will spur anti-spam vendors to provide better integration and management of Microsoft's and other vendors' email client/server platforms. ■