



In the security arena, things can change fast. EAMON McGRANE investigates the impact on firewalls, anti virus and IPS

Security was never really a chicken and egg or, indeed, a horse and cart scenario – it was easier than that. First came the virus/vulnerability then the signature, patch or definition.

That situation has, however, changed somewhat. The shift in direction of malware writers from computer savvy nerds with attitude to Soprano-like cyber gangs has led to attacks becoming more sophisticated, targeted and exacting.

Security had to respond. The firewall, once the bastion of internet security, has become unsteady on its feet under the new styled attacks. Anti virus, anti phishing, anti spyware and anti spam are now all deployed in conjunction with the firewall to keep unwanted traffic out. But these components' main weakness is their reliance on updates, patches and definitions of new threats and

dangers.

Zero day

With the shift in attacks, zero day protections have become popular by using a mixture of pattern analysis and behaviour to identify possible danger, before a patch/definition is released. In addition, unified threat management (UTM) devices are demonstrating versatility as an all in one defence. The question then is, who is buying solutions such as zero day and who is sticking to the blended multi-vendor approach in securing their endpoints.

"IPS and zero day through a UTM device is taking on what was traditionally the firewall but now it adds a lot more such as intrusion detection and prevention," said Colin Reid of Topsec.

Reid believes a blended approach works best as you're not "putting all your eggs in one basket".
"We have customers who might have a Watchguard UTM, they have anti virus, anti spam on the intrusion

detection/prevention system (IDS/IPS) but they might have Symantec anti virus on their network as well as on their desktops or servers. And we would recommend that

because there's always going to be something that one vendor will miss and another one would pick up. In a large network we'd recommended the blended approach but in an SME it'd be fine to go with just one box such as UTM."

Early adopters

Conor Flynn of security consultancy Rits said the early adopters such as the financial institutions are the ones

looking at UTM and blended technologies. "This sort of technology is still in its infancy

and would require people to have a leap of faith in using it. So the early adopters are

taking them on trial in conjunction with more traditional products. I haven't yet seen anyone who'd be prepared to replace their existing signature-based technology with the more heuristic or pattern based approach."

Flynn said it would require a mind set change from people who are working with more traditional technologies because up till now everything has been about getting your signatures updated, waiting for the attack and defending against it when it comes with the solutions from the vendors. "That's not really a good approach anymore and perimeter based solutions aren't enough because security has to be taken back to every node in the network," he said.

Human resource

One of the trickier parts of implementing solutions such as IPS, Flynn argued, is the initial overhead from a human resource perspective. "You're going to have to make sure your people are highly trained and they're going to have to spend a lot of time responding to false positives and negatives. You have to tune the device so it

doesn't stop valid traffic and grind your business to a halt. And that's something a lot of companies don't prepare for.

"We saw companies implementing IDS evolving into IPS and they've ended up gathering dust on the shelf

and not being used because the resource overhead to manage them was so high. Now that resource overhead tapers off...but once you've tuned the system the overhead drops off but

it will pick up again if you introduce new network traffic or applications that could appear anomalous, so you will have to retrain the device."

"What we're finding is that in the SMB side of the market there's single UTM boxes going into those customers rather than multiple services," said Justin Owens of Commtech. "In larger customers such as medium enterprise up, there are point solutions going in. And some of that has to do with speed and capability. Generally what people say with UTM boxes is that you're

getting 80% of the functionality for 20% of the price compared to point solutions. But in the mid enterprise market up, 80% of the functionality isn't enough."

Best of breed

Owens said bodies such as government or financial institutions are looking for best-of-breed with more capability built into the point solutions with firewalls now going up to the application layer. "So rather than just allowing web traffic through, these firewalls actually understand the traffic as well and can see if there's malicious content there."

Owens said Commtech is seeing companies in the enterprise space tending to go for application layer firewalls. "Most of the

banks have them and we notice that those kinds of organisations are using them to inspect web traffic.

They might be using boxes such as Bluecoat, a product that's fast and mostly single purpose but it will do content filtering, spyware and even AV but it is not a full UTM box that does everything - it's a subset of a UTM device and that's the way we think it'll keep going. We don't see that people will have a single box in the enterprise space."

Enterprise needs

Owens feels that this trend will continue with large enterprise using best of breed

point solutions with SMB going for standalone UTM devices. "For SMBs it's more cost effective and they are much less complex. So for companies that don't have an IT person in-house it's a preferred option to having multiple solutions with all their attendant administration problems and costs. Here they have one single product that does everything. And as long as they keep the licenses up-to-date it's pretty much zero touch-it updates itself in real time while protecting you against zero day vulnerabilities." ■

IPS and zero day through a UTM device is taking on what was traditionally the firewall'

We saw companies implementing IDS evolving into IPS and they've ended up gathering dust on the shelf because the resource overhead to manage them was so high'

ICT Advisor

In this month's ICT Advisor we look at the security stalwarts, firewalls, anti virus and intrusion prevent systems. These perennials have developed at a phenomenal rate in response to threats of late and we examine the current state of the art and where they are going.

Value Points

- ∴ **Implementers:** The market is seeing convergence but large enterprise still favours layered security and point solutions
- ∴ **Vendors:** While zero day protection reduces reliance on signatures, frequent signature updates will be necessary for the foreseeable future for most security products