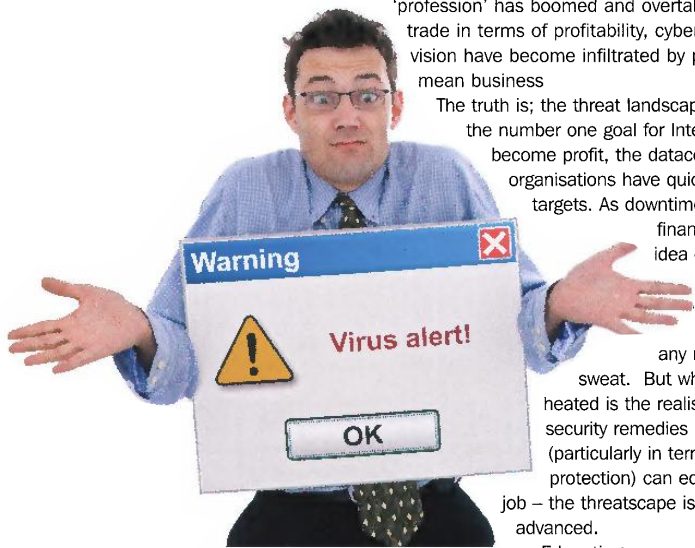




# The AV arms race

## – staying one step ahead...

**Risk UK talks to Paul Judd, Regional Director for UK and Ireland, Fortinet about the role of anti-virus technology in keeping one step ahead of attackers**



Long gone are the days when cybercriminals targeted their prey at random, aiming only to wreak havoc simply 'because they could'. As the 'profession' has boomed and overtaken the drugs trade in terms of profitability, cybercriminals' fields of vision have become infiltrated by pound signs. They mean business

The truth is; the threat landscape has evolved. As the number one goal for Internet crime has become profit, the datacentres of large organisations have quickly become prime targets. As downtime equates to huge financial shortfalls, the idea of letting any hackers onto a corporate network is enough to make any network manager sweat. But what gets them really heated is the realisation that keeping security remedies updated (particularly in terms of antivirus protection) can equate to a full time job – the threatscape is just that advanced.

Educating users and updating security solutions and policies to keep pace with new and evolving viruses has resulted in a real arms race. To avoid being outrun by criminals, enterprises need to deploy the most advanced and comprehensive defences in order to protect their assets and business-critical data.

Viruses used to be the primary concern that was enough to make network managers squirm, but viruses can no longer be treated as a standalone threat. The virus landscape is evolving at such an exponential rate that as soon as a patch for one virus is formed, another version of the virus can instantaneously break out. On top of viruses evolving and morphing into new forms to bypass the latest in threat protection, enterprises are being faced with more and more blended threats - combining attack characteristics from different malware categories such as Trojans with embedded spam engines, or viruses with spyware payloads - that have the potential to cause unprecedented harm to business.

Nowadays, AV solutions are inefficient on their own unless they have the intelligence to understand more than the makeup of just viruses i.e. application exploits, spam, DDoS, worms, phishes etc. Many of today's prominent threats begin in a traditional virus 'format' but can lie dormant when seemingly cured. These viruses can then go on to establish connections with 'command and control centres' to join forces in launching DDoS attacks or generating spam traffic – and this is where things get messy. Advanced, blended threats have the power to bring down organisations' IT and web systems

quickly and simply, and all without user interaction.

Without addressing fundamental IT security issues that are crucial to any business, enterprises can also find themselves on the wrong side of the law. More than the misunderstood and distant threat of nasty viruses ever could, compliance is putting the wind up the boardroom bigwigs. Yet you can't just install an AV filter to put a tick in the compliance box; if only it were that simple. Legislation means that failing to take IT security seriously enough and fulfilling adequate reporting duties can not only drastically affect the business and its customers, but individuals within the organisation can also be found liable. If employers fail to meet governmental standards of compliance by putting the adequate IT protection in place for example, they may be deemed reckless and in breach of the 'duty of care' they uphold for their customers and employees.

So, while it is clear that security is about more than just AV, it's about comprehensive and intelligent defence, one might ask: what does this mean in terms of complexity and cost?

Pressure is mounting and it is clear that large enterprises have a battle on their hands, but it needn't be an uphill struggle. Choosing to layer their networks with standalone security solutions in a desperate attempt to plug holes in the armoury is a costly and ineffective strategy. Piecemeal, reactive security solutions are giving way to strategically deployed, integrated multi-threat security systems. Instead of having to install, manage and maintain disparate devices, organisations can consolidate their security capabilities into a commonly managed appliance.

Rather than blocking a virus and forgetting about it or starting a new chapter in the security system every time a new evolution of threat appears, having a security set-up that shares multi-disciplinary knowledge in the first instance can mean viruses are prevented from developing into various other forms of serious threat. This proactive approach to defence is far more favourable than being forced to be reactive, and dramatically reduces management complexity and deployment costs.

### Adding extra capabilities

Every chance you have to add more capability to your defences presents an opportunity to reduce your hardware; and with it the expense of excess management overhead power and space. Consolidating your security is an appealing proposition, especially when the by-products equate to increasing security enforcement and effectiveness.

If businesses look to the real experts in this space - I'm talking the guys that are dedicated to monitoring these sorts of security developments on a 24x7 basis - the burden can be instantaneously lifted. Consolidated multi-threat security solutions that protect against all known and unknown threats are never complacent, and are dedicated to improving their defence systems on a continual basis. When threats appear or are identified during an early stage of development, integrated multi-threat security systems can be automatically updated with relevant patches or defences for all functions from AV, firewall and web filtering to antispam, so enterprises can continuously be protected.

If enterprises invest in these sorts of future-proof solutions, throwing dead money at resolving security issues will be a thing of the past.

*If enterprises invest in future-proof solutions, throwing dead money at resolving security issues will be a thing of the past*