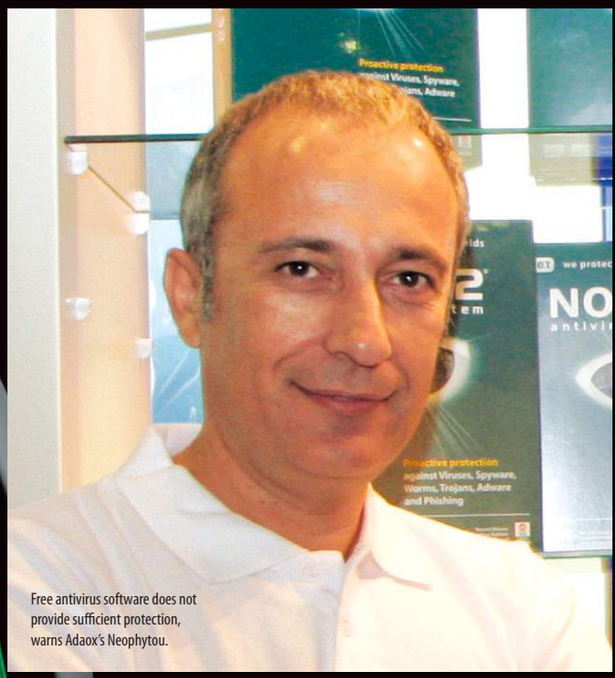
January 2011 Vol.17 No.01

Defensive measures

With an ever-changing threat and malware landscape to contend with, network managers in the Middle East need to take an integrated approach to the way they deploy antivirus software solutions. Piers Ford reports.



Free antivirus software does not provide sufficient protection, warns Adaox's Neophytou.

> We have been saying for a long time that having an antivirus-only solution on endpoints is not enough. Stuxnet has proved that this is very true

The arrival of Stuxnet is a wake-up call for any network manager who still thinks a batch of antivirus software licences running on a host of end-user devices is enough to ensure protection against a rising tide of malware.

The security industry has been united in its assessment of this particularly virulent worm, apparently designed specifically to target industrial control systems: with its complex, multi-level framework, it marks a watershed in malware evolution. The entire infrastructure is at risk these days.

As cyber crime rises in the Middle East, IT decision-makers should be taking a long, hard look at how antivirus technology integrates with their complete security strategies.

"The landscape is changing rapidly, that's for sure," says Bulent Teksoz, channel technology officer for emerging markets at specialist security vendor Symantec. "The game has changed. We've been saying for a long time that having an antivirus-only solution on endpoints is not enough. Stuxnet has proved that this is very true. In order to truly protect their organisation, IT managers need to employ solutions that can provide protection at multiple layers. Our latest internet security and threat report shows that cyber crime has been shifting to emerging regions such as the Middle East. This brings additional risk for IT managers here," he warns.

Mahesh Vaidya, CEO of data storage and security solutions provider ISIT Middle East, agrees that cyber crime is a growing problem in the region, and says IT managers need to take a holistic approach to internal system protection.

"Traditional antivirus solutions are just not enough," he says. "Antivirus software should be complemented with device and patch management, device control, encryption, data loss prevention and so on. It is only a small part of the security landscape. IT managers should be looking at solutions and systems integrators that give more comprehensive protection at different levels, but also better manageability and ease of use."

All of which means that those 'free' antivirus downloads which product vendors offer as part of their hardware package, and which might superficially tick a box on the security checklist, will usually fall far short of addressing the real requirement.

"Free antivirus software doesn't provide contracts, SLAs and support, and it will be the installer's responsibility to maintain it," says Waseem Hattar, IT security manager at managed hosting and IT security provider eHosting Datafort.

"Antivirus solutions require a lot of investment in terms of people and infrastructure to respond to attacks immediately, and free antivirus software will find it difficult to sustain the quality of the product — good people and infrastructure don't come free of cost!" warns Neo Neophytou, managing director at security vendor ESET's regional business development centre, Adaox Middle East. "Free solutions have limitations as they

Case study: ADCB

Abu Dhabi Commercial Bank (ADCB) aims to be the number one bank of choice in the UAE, but has always understood that it can only achieve its goal by adhering to the most rigorous security standards, meeting compliance requirements — particularly in the payment card industry (PCI) — as well as customer expectations that their transactions will be safe.

"Because ADCB is growing so fast and introducing so many new services, the challenge is to keep up with the latest market trends from a banking perspective in the most secure way possible," explains Steve Dulvin, head of IT operations.

When the bank decided to overhaul its existing, heavily manual approach to security management, it looked to its existing investment in Symantec Antivirus as the foundation for more effective control of its endpoints. It now has a fully integrated security model, in which antivirus software is a lynchpin rather than a standalone tool.

End-point Protection combines firewall, antivirus, intrusion protection, and application and device control technologies, delivering advanced threat prevention and robust defence against malware for the bank's laptops, desktops and servers. These were previously managed manually. The centralised approach means that software and policy updates and reporting can now be controlled from one place under a single licensing and maintenance programme.

"Using Endpoint Protection we benefit from reliable, automated protection, and can proactively enforce the operational security we need," says Dulvin.

Symantec's Teksoz says network managers need to establish a solid, integrated solution with multi-level protection.

Companies need to consider the frequency of signature updates when assessing antivirus software solutions, advises eHDF's Hattar.

don't provide any kind of support and it isn't advisable to rely on a security solution like that. It is always better to invest in security — not react after an attack has taken place."

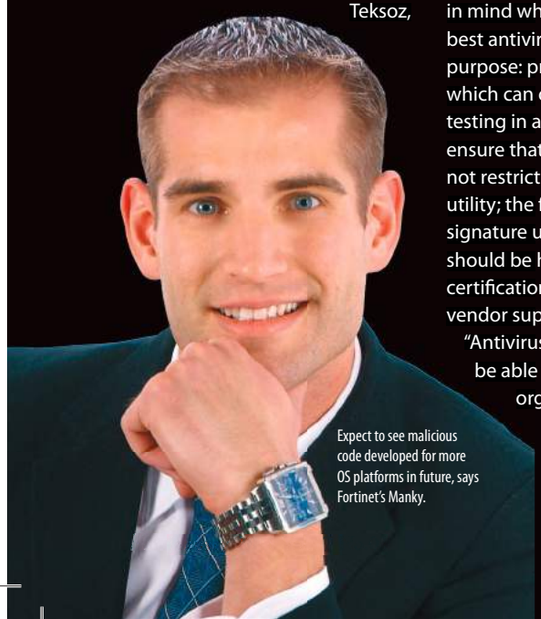
Neither is it enough to install an off-the-shelf antivirus package and stand back in the assumption that everything has been taken care of. Deployment should be closely integrated with security policies, device management and properly patched operating systems. Antivirus can no longer be seen as a standalone solution.

"Installing an endpoint solution is a great step in the right direction," says Symantec's Teksoz, "but they have to be managed properly as well. That is not to say IT staff have to spend hours a day managing the solution, but rather there should be periodical checks so they know the network is protected all the time. This can only be achieved by installing the right solution in the right way."

And that means deployment should be planned in a more informed way, taking into account the rate at which malware is being unleashed on a constant basis, as well as the scope and scale of the organisation's network.

At eHosting Datafort, Waseem Hattar says IT managers should bear four main considerations in mind when selecting the best antivirus software for their purpose: proof of concept, which can only be realised by testing in a live environment, to ensure that the software does not restrict server or network utility; the frequency of antivirus signature updates, which should be high; security agency certification; and first-class vendor support.

"Antivirus software should be able to protect the organisation from new and unknown threats, as new viruses and worms are



Expect to see malicious code developed for more OS platforms in future, says Fortinet's Manky.

A decade under fire

The first decade of the 21st century has seen corporate IT systems bombarded by a staggering array of increasingly powerful, intelligent malware, from the I LOVE YOU worm (2000) to 2001's Code Red Worm, Beast Trojan (2002) all the way through to Stuxnet.

While the perception has always been that all you need is the protection of a reliable antivirus software licence from a vendor who is shouldering the hourly burden of detection, a quick look at how pernicious these viruses have become makes it clear that for just about any type of organisation, antivirus software should be a fulluy integrated element of the overall IT security strategy.

"Stuxnet is quite a devious framework as it presents a certain level of multiplicity," says Derek Manky, project manager, cyber security and threats research at network vendor Fortinet's Fortiguard Labs.

"More specifically, it consists of an 'exploit' part, a 'Rootkit' part, involves specific infection vectors, targets a specific class of victims [industrial control systems] and has unusual characteristics, such as software certificates that seem to have been stolen from a well-known hardware producer.

"Since 2009, we have seen more threats arising that target different platforms such as SymbianOS, Blackberry, Android and Simatic WinCC/STEP 7. Early in the decade, threat developers were focused on creating frameworks and malware that we see in today's modern botnets that operate primarily on Microsoft Windows systems.

"While some developers will continue to stay on the Windows platform over the next few years, expect to see a growing demand for malicious code on growing platforms such as those used by smart phone manufacturers and cloud computing providers."


Antivirus solutions need to be supplemented with other security technologies, suggests ISIT's Vaidya.

generated on an hourly basis," explains Neo Neophytou at Adaox. "The software should also be light on resources, it should be easy to deploy and manage, and ideally it won't clog the network bandwidth."

The size of the organisation is an important factor in making the right decision — SMBs will favour simplicity and ease of management, while large enterprises will probably look to a centralised solution capable of managing multiple sites and locations. It could also have an impact on the proportion of IT security budgets that should be spent on antivirus software.

Large organisations will typically spend 10% to 15% of their security budget, but SMBs will set aside as much as 35%, according to Neophytou. It all depends on a careful assessment of the value of critical data and the potential impact of its loss on the business.

"The challenges faced by larger enterprises could be different from those of SMBs," says ISIT's Vaidya. "For example, if the companies have a mobile workforce, remote offices and are using cloud services, the traditional corporate security boundaries might have to be redefined and more comprehensive security policies and technologies implemented."

Teksoz at Symantec agrees that the more complex the network layout of a company, the more thought should be put in to the design phase.

"Large enterprises usually have no boundaries at all, thanks to wireless networks, cloud computing and remote workers," he comments. "This means they have to take multiple risk factors into consideration. It isn't the antivirus software, but the endpoint protection solution that needs to be in every security budget. It is about having a solid, integrated solution with multi-level protection, ease of manageability and use. There are not many solutions out there that can offer this level of protection," he concludes.