Title:
Security: The Hardware Advantage

Word Count:
942

Summary:
Malicious Code attacks & E-crime at the gate: Software Security Solutions Are Just Not Good Enough!

Keywords:
Software, Security, Hardware, Advantage, firewall, antivirus

Article Body:
A fairly high percentage of computer users are now educated enough to know they must have security products deployed in order to protect their computers.
In the case of Corporate Users, the IT staff makes sure their gateway is stacked with the latest and greatest security appliances protecting the parameter.
In the case of Home Users, the users themselves make sure to install security software, typically a combination of personal firewall, antivirus and anti-spam. Or a single streamlined Internet Security Suite.

In both cases, the solution is simply not good enough!

We'll start with explaining why security software running on top of the computer it aims to protect will always be inferior to an external hardware solution. The following points are well known to the IT professionals as they would obviously never rely on software installed on users' computers alone, and will always focus on the hardware-based security appliances protecting the organization's perimeter.

The advantages of external hardware-based security appliances are:

Immunity from the inherent vulnerabilities of the underlying OS – If, for instance, an organization is running MS Windows on all its computers, the security software installed o the computer will still suffer from the same underlying vulnerabilities and backdoors that Windows inherently has. When you are protected by an external appliance who has its own proprietary OS (Or a flavor thereof), the security mechanism does not suffer from these vulnerabilities.
Mobile code is not run - content arriving from the internet is not executed on

these appliances it just goes or does not go through into the network. It makes it more difficult to attack as the mobile code delivered by the hackers does not run on the appliances.
Cannot be uninstalled – Security attacks often start by targeting the security software, while trying to uninstall it or stop its activity. Software-based security solutions, as any software program includes an uninstall option that can be targeted. In contrast, the hardware-based security appliances cannot be uninstalled as they are hard coded into the hardware.
Non-writable Memory - Hardware-based solutions manage the memory in a restricted and controlled manner. The security appliances can prohibit access to its memory, providing greater protection against attacks on the security mechanism.
Controlled by IT personnel – The security appliances are controlled by IT, who constantly maintains the highest security policies and updates.
Performance - The security appliances are optimized for maximum security and operate independently from computers in the network, not degrading the performance of the desktops or consuming their resources.
Prevent potential software conflicts – The security application you install on your computer will reside on the same computer with an unknown amount of other unknown software all using the same CPU, memory, OS and other resources. This often results in various conflicts, “friendly fire” between 2 or more unrelated security application installed on the same computer etc. When using a dedicated hardware security appliance, nothing runs except for the intended use it was made for.
These are all just the general conceptual problems of protecting a computer with the exclusive reliance on an installed software security application.
There’s a lot more to be said about the problems with these types of solutions. The lack of Network Address Translation (As you’d get in a dedicated external hardware-based security appliance), lack of physical network separation (DMZ), the fact that even simple ARP poisoning attack cannot be stopped by them and much, much more.

Now that we’ve clearly established that using software-based security applications is not the best security solution – what’s wrong with the security that Corporate Users get? The IT staff makes sure their gateway is stacked with the latest and greatest security appliances protecting the parameter.
We’ve shown that that would be the best way to go – So where is the problem?

The answer to that is simple – Mobility.
More and more of the corporate users actually have laptops and no desktop computers. More and more users are becoming mobile, working remotely from outside the organization, working either from home, or are simply on the road traveling as part of their business duties.

The minute the user packs up his laptop and leaves the protected (by a series of

dedicated hardware security appliances) organizational perimeter – all the amount of money and professional effort that went into building up the corporate gateway, all of that becomes meaningless!
The user has left the corporate protection behind, and is left essentially "naked" only with the software security solution to his protection. And we've already established above it is not enough.

So what is the perfect solution?

The perfect solution that solves all the issues presented above is simply to use a Personal Security Appliance – A term coined by Yoggie Security Systems. Yoggie has coined the term and essentially created a whole new category of security products. The first of its kind in the world is the Yoggie Gatekeeper which is a powerful and robust hardware-based security appliance that connects to the laptop and externally scans and protects all the traffic with a series of 13 different security applications.
The Yoggie Gatekeeper is tiny and mobile, fits comfortably in your palm and can simply be attached to a USB port on your laptop, which provides both the power and connectivity.

This way the powerful corporate-level security can be re-instated even as the user is away from the protected corporate perimeter, allowing the laptop user maximum performance and productivity (by offloading it and using external security applications, instead of laptop-installed ones), giving them the highest level of security, and allowing the IT department means to monitor and enforce security policies over remote and traveling laptops without being intrusive to their users!