Title:
Outside the safe zone

Word Count:
1015

Summary:
This document presents the advantages of a hardware-based security appliance over
a software based solution.

Keywords:
mobile, wireless, Security, Hardware, firewall

Article Body:
Businesses around the world are being bombarded with sophisticated threats against their data and communications networks every day.
As enterprises invest heavily in fortifying their IT infrastructures and enforcing comprehensive and constantly upgraded security policies against malicious code attacks, another home-grown threat - the mobile workforce - is opening the floodgates to compromised enterprise data and corporate network contamination.

Though mobile working offers gains in commercial and operational value, enterprise security policies often stifle the effectiveness and productivity of mobile workforce devices.

Here we examine why best of breed softwares, in isolation, are not able to provide the mobile workforce and their laptops with the same high level security afforded to office based workers.

Two lines of defence in a protected corporate environment
Currently organisations anticipate, detect, and prevent threats from laptops attacks via a layered approach.
This is coupled with centralized, uncompromising IT policy which overrides an individual’s control over his/her own laptop.
As IT departments prioritise corporate IT governance, their primary method of effectively enforcing organizational security policies is by controlling all networking components.

When connecting to the Internet from within the corporate network, laptop users

are protected by two lines of defence:

A comprehensive set of IT security appliances running secured and hardened Operating Systems, and security software including firewalls, Intrusion Prevention/Detection System, antivirus, antispyware, antispam, and content filtering, all of which are completely controlled by the respective corporate IT organization.
Personal firewall and antivirus software installed on the user’s laptop and controlled by the user.
In addition, when laptops are within the protective corporate environment, the organization’s IT department can exercise full and consistent control over (and visibility of) any device, which is a critical operational consideration. This means the IT team can:

consistently update respective laptops with data, policies, etc.
monitor the entire network effectively vis-?-vis the status of all network components.

Outside the safe zone
Once a laptop starts 'roaming' outside the enterprise governed network, the 2-line defence system no longer applies, as the laptop is essentially no longer protected by the corporate security appliances layer, and is exclusively dependent on the security software installed on the local operating system.

The roaming laptop is exposed to potential threats from nearby wireless and wireline devices (in hotels, business lounges, airports, WiFi at Internet Cafes, etc.).

These threats signify a danger far beyond the scope of the individual laptop, as intrusive code may proceed to use the laptop as a platform for breaching corporate security, once the laptop had returned to its base, and is connected to the network.

Relying solely on the best of breed software on the laptop is flawed due to:

Operating System Inherent Vulnerabilities - by definition, security software running on Windows is subject to inherent Windows vulnerabilities, effectively exposing personal firewall and antivirus applications to malicious content attacks.
Unknown Threats – the security software can only defend against known threats. By the time these threats are added to the knowledge base, it may be too late.
Immediate Damage - malicious content executes directly on the platform to be

protected, rather than on a security appliance designed to filter the content and serve as a buffer.
Managing Security Level – making sure all the computers have installed the latest security updates and enforcing a unified security policy can be very difficult. When the computers themselves are at the frontline, these security weaknesses can be disastrous to the entire network. In other words, it's "all or nothing", either the entire network is secured or nothing is secured.

Consequently, many organizations adopt tough security policies prohibiting most wireless networking options (significantly limiting user productivity and remote computing freedom), or imposing strict, costly and difficult to enforce cleansing procedures for laptops that return from the "field".

Best of breed software made mobile
A growing number of CSOs have decided to place computers behind a robust security gateway, usually a dedicated security appliance, to counteract the current weaknesses in laptop security.
Unlike PCs, these appliances are equipped with hardened operating systems that do not have security holes, "back-doors", or unsecured layers. They are designed with a single purpose, to provide security.
The fact that these security appliances are hardware-based and not software-based provides the following advantages:
Cannot be uninstalled – security attacks often start by targeting the security software, and trying to uninstall it or to stop its activity.
Software-based security solutions, as any software program includes an uninstall option that can be targeted.
In contrast, appliance-based security cannot be uninstalled as it is hard coded into the hardware.

Non-writable memory - hardware-based solutions manage the memory in a restricted and controlled manner. Security appliances can prohibit access to its memory, providing greater protection against attacks on the security mechanism.
The use of hardware allows the combination of a comprehensive set of security solutions in a single device.
Hardware also allows the combination of best-of-breed enterprise-class solutions with proprietary developments working on both the lower and higher levels (e.g. packet and network level, application level etc.).

In addition, the well known tension between users and IT managers over their computing freedom can be overcome via hardware.
On one hand, users want to have complete freedom when using their computers, while on the other hand, IT managers try to enforce security policies (e.g.

banning the use of P2P software).
By using a security appliance, IT managers solve the conflict between the user's desire for computing freedom and the IT manager's desire to control and enforce security policies.
With software, policy is part of the laptop or computer, whereas through an appliance security policy can be enforced outside the laptop and the user has complete freedom inside the safe computing environment.

In conclusion, to provide corporate level security for laptops operating outside the safe office environment, CSOs should consider layered security architecture on a hardware appliance.
A dedicated appliance can hold all of the best of breed security softwares, and is able to re-introduce the two lines of defense enjoyed by office based PCs.
By introducing a security gateway, should security be breached, the damage stops at the gateway.