



Home page (<http://www.wi-fiplanet.com/>):

News

[Senforce Unveils Mobile Firewall](#)

[September 27, 2004] This new software takes the company back to its roots in securing mobile devices but this time using policy enforcement.

[Wayport in Patent Suit](#)

[September 24, 2004] A 'patent apocalypse' may be arguable, but infringement suits are hitting all areas of the Wi-Fi vendor community with this latest announcement. Even those that have settled sometimes appear far from over for all parties.

Etc.....

News item (<http://www.wi-fiplanet.com/news/>):

News

Senforce Unveils Mobile Firewall

By [Ed Sutherland](#)

[Senforce Technologies](#) has released its Senforce Portable Firewall Plus (SPF+) for mobile devices. The software takes control of laptop computers at the network level, enabling users to shut off wireless connectivity, control access to hotspots and ensure computers are equipped with the latest virus protection.

SPF+ is based on the same key technologies found in the Senforce Enterprise Mobility Manager: AccessAware, LocationAware and Quarantining. Unlike its big brother, SPF+ takes some of the decision-making out of the hands of users.

"Because other products were built for consumers and not for businesses, they ask the users to make security decisions, often resulting in the user disabling the product altogether," according to Senforce.

"This is not a one-size-fits-all world," says Tanya Candia, vice president of marketing at Senforce.

"The real strength of SPF+ is that it operates at the lowest level possible," says Candia. It understands the Network Driver Interface Specification (NDIS), a Microsoft invention making life easier for network interface card developers.

By using a firewall based at the NDIS layer, business IT departments can control the Wi-Fi card in laptops, restricting which wireless sources are available to users. SPF+'s AccessAware feature takes in to account a Wi-Fi signal can emanate from a secure corporate WLAN, a public hotspot across the street or a neighbor's wireless home network.

"Securing users at the application layer is leaving users and businesses vulnerable to security breaches and the loss of countless hours and dollars," said Candia.

SPF+ can also restrict which Wi-Fi signal is used by wireless employees. Often, wireless laptops will try to keep connected to the strongest available signal — be it a secure corporate WLAN or the coffee shop across the street. SPF+ can remove all connection options except for the company WLAN, says Candia.

Other firewalls "check virus definition files for updates only when a system reconnects to their network," Senforce's SPF+ employs "Quarantining," which forces a user to update virus software. Until the anti-virus software is updated, a user will see only a blank screen with a link to their anti-virus vendor, says Candia.

Wireless is the biggest security risk posed by laptop computers, she claims. Unlike firewalls protecting traditional wired networks, security is much more challenging in an increasingly mobile workplace. You don't know where or when mobile workers will connect to an office network.

Candia points to the growing number of mobile employees working from home and telecommuting. Senforce's SPF+ provides mobile users with three default configurations: home, work, or alternate. The alternate configuration can be customized allowing you to work on the road and connect to the corporate network via public hotspot.

"With SPF+, my mobile workforce doesn't have to worry about security — we are protected no matter where we go, and it prevents the type of attacks that continue to plague other small business," said Joanne Ireland, president of Ireland Presentations, a San Francisco-based event planning business.

"SPF+ has lowered my office's down time, lowered my operating costs and almost importantly, my frustration level," says Ireland.

The software sells for \$34.99.

September 27, 2004