

---

# Linux Security from a Windows Security Expert's Perspective

Posted by Dave Wreski  
21 September 2000

In this interview, Avi Fogel, CEO of Network-1, offers his perspective on the state of Internet security, his experience with Windows and security, and the advantages and disadvantages to Open Source security.

Recently I got an opportunity to speak with Avi Fogel, CEO of Network-1 Security Solutions, Inc., an industry-leading developer of distributed firewalls and other security products primarily for Windows platforms. I thought it would interesting to speak with an established security expert that addresses Internet security from the Windows and closed-source perspective, and see what his views are on topics including Open Source, Linux, and the current state of security in general.

LinuxSecurity.com: Can you describe a bit about your background? How did you get involved with security? What did you do prior to becoming the CEO of Network-1?

Avi Fogel: Like many in the security industry, I grew up in a security conscious environment -- in Israel. I graduated from Technion, the Israeli Institute of Technology, with a degree in Electronic Engineering and served as technical officer in the Israeli Defense Forces. I have come to network security from computer networking in which I've been involved since 1980.

Prior to coming to Network-1, I was president, CEO and co-founder of CommHome Systems Corporation, a residential networking startup. I also held positions as vice president of global marketing at Digital Equipment Corporation - Network Products, executive vice president of global marketing with LANNET, Data Communications, Ltd., a LAN switch manufacturer and president and CEO of LANNET America.

When my startup company, CommHome Systems, was acquired by the investors of Network-1, I was brought aboard as President and CEO of Network-1.

LinuxSecurity.com: Can you give us a brief overview of the products and services you offer at Network-1? How does your packet filtering firewall differ from other firewalls? Can you explain some of the basic concepts of packet filtering?

Avi Fogel: Our strategic products and the ones that give us the greatest market differentiation are distributed, host-resident firewalls for servers, enterprise-wide personal computers and workstations. These are CyberwallPLUS-SV (for servers) and CyberwallPLUS-WS (workstation), respectively. Presently, we address the Windows NT/2000 market, but do plan to expand into other platforms. In an unpublished report by one of the major market analysis firms they indicate that distributed host firewalls will become a \$250M market by 2004. Network-1 believes that it has advantages in depth of security, especially in server environments, in performance and in management abilities

vs. other players in this area.

To round out our product offering and to offer protection for other platforms, we offer CyberwallPLUS-IP as a perimeter firewall and CyberwallPLUS-AP as an internetworking firewall for LANs. Although these too are for Windows NT/2000 servers, they offer protection for heterogeneous networks.

To manage it all we provide CyberwallPLUS - Central and CyberwallPLUS - Remote, for remote monitoring and control of the distributed firewalls in a network.

LinuxSecurity.com: What do you see as the most significant trends or developments in computer security in the next few years?

Avi Fogel: The emergence of the distributed, host-resident firewall for open, e-business networks is making headway. Analysts are investing in researching the size of this market and industry pundits are writing about this area as the next generation of Firewalling technology. We recently announced an enterprise-wide sale of our workstation product, the WS edition, to BMC Software and have had an important subsequent one to a major government agency. We are seeing similar enterprise-wide opportunities come up for Windows workstations and servers in many segments - government, industry, education and financial institutions. These are better able to secure all the various access points in the open environment presented by e-Business, than the traditional packet-filtering router and perimeter firewall approach. They also scale upward in growing networked environments predictably without the performance degradation you are likely to get from traditional approaches.

LinuxSecurity.com: What do you think of Linux as a viable platform for developing security products? Has Network-1 given any thoughts to developing security software for Linux?

Avi Fogel: While there are some differences in vulnerabilities between OS's and the availability of shareware to address these - Linux, like Windows and traditional Unix suffers from the lack of granular Network Access Controls and built in Intrusion Detection and Prevention capabilities and capabilities for extensive logging of network transactions. Network-1 sees Linux as a very important platform that we want to be able to address in the future as part of a full host-resident distributed firewalling solution.

LinuxSecurity.com: Do you think Linux has a place in the data center as a secure platform for commerce in the state that it's currently in?

Avi Fogel: Due to the greater availability of applications for Windows and Unix today they may be better suited for these services today. I see Linux as a great candidate for a future capture of market-share on the desktop away from Microsoft. It is also a great tool environment for infrastructure software and hardware solutions - for appliances and for all-in-one SME solutions (Firewalling, VPN, management, VoIP, etc.). The investments of the big system vendors (IBM, Dell) and Sun Micro (with Cobalt) will make Linux a major contender in the data center, down the road.

LinuxSecurity.com: What are some of the biggest challenges you face when dealing with security?

Avi Fogel: It's an organic situation. The hackers represent everything from the genuinely intellectual curious to undisciplined script kiddies. The only constant is that their threats are constantly changing to overcome network defenses as they grow more numerous. The major problem with network security in general is the fact that it is still considered by many IT managers as a fringe issue - and is still in the category of black magic - a little understood phenomena of IT systems and networks. The nature of network security is also about continuous discovery of new holes and bugs that pose security threats.

Thus the general problem is that of a need for continuous education by the network security vendors to get high enough on the attention span of IT decision makers.

LinuxSecurity.com: What do you think can be done about denial of service and distributed denial of service attacks? What do you think is the most significant threat to the general Internet community today? What will it take to resolve these issue?

Avi Fogel: Enterprises need to step up and show due diligence in implementing sound security for their networks. If for no other reason -- to keep from getting sued when their sites are used as launch pads to bring down an eBay or Amazon. The threat will focus on the lowest common denominator -- those sites with high speed connections and limited or no protection will be hit first and most often. Diligence on the part of enterprise web site owners and even the home user with high speed connections is a good start for the overall security of the Internet. Adding egress filtering technology and mandating its use on hosts, firewalls and routers would prevent the use of machines as zombies of DDoS or Trojans.

LinuxSecurity.com: Can you make any comparisons between security of UNIX versus the security of Windows? How much do you think the maturity UNIX has an effect on its overall security?

Avi Fogel: UNIX and Linux have slightly better network address filtering capabilities than Windows and Unix has better online help as it relates to network security. Unix and Linux also have more shareware tools to address some of the issues that host-resident firewalling addresses, such as logging tools. Generally though all OS's lack network access controls and intrusion detection capabilities.

LinuxSecurity.com: Do you believe the open source nature of Linux provides a superior vehicle to making security vulnerabilities easier to spot and fix?

Avi Fogel: Definitely yes. On the other hand open source means easier to crack through well known bugs and deficiencies and a lot of free code that could itself be a tool made available by hackers. Users need to be aware of the latter threats and closely and timely monitor vulnerability notifications and carefully check the source of code they use.

LinuxSecurity.com: I'd like to thank you for your time today, and sure appreciate the opportunity to speak with you. We look forward to hearing of new developments on your work in the Linux security market!