

Outpost Network Security 2.0

Outpost Network Security (ONS) 2.0 is a comprehensive security solution designed to provide centralized, easy-to-manage protection for small and medium-sized businesses and branch offices against the latest intrusion threats and malware attacks. ONS provides proactive endpoint protection against inbound attacks and outbound information leaks in conjunction with powerful anti-spyware defenses to deliver high levels of protection for business operations with limited IT resources.

ONS functionality includes:

- stateful bidirectional firewall
- proactive (blocking) and reactive (signature scanning) anti-spyware
- centrally-managed event deployment, management and updates
- customizable settings for different user groups within the organization

Outpost Network Security can be deployed across the network to all or selected workstations and managed from the central administrator's console. Automated, always-on protection ensures employee computers stay secure and operating smoothly, while the centralized administration keeps IT demands overheads at a minimum.

Security and Privacy

- Always up-to-date, automated spyware protection prevents infection and keeps machines running smoothly: the active monitor blocks new infections, while the on-demand scanner removes any traces of existing infections.
- Targeted data protection prevents confidential corporate information from ever being sent off an Outpost-protected workstation.
- Client firewall starts protecting endpoints as soon as it is installed by continuously monitoring all data traffic and automatically dropping unauthorized connections.
- Client machines are rendered invisible on the Internet so hackers cannot 'see' and exploit them.
- The Attack Detection module prevents known and unknown attacks on protected workstations, optionally alerting the client.
- Unique Ethernet defense prevents internal network tampering and blocks client-based attempts to disrupt or disable wired or wireless network communication.
- Administrator-assigned application rules govern client machines' Internet access policies.
- Embedded code defense mechanisms prevent malicious applications from activating under the guise of a trusted application, protecting clients from advanced application injection and spoofing techniques.
- Active web content module blocks installation and activation of malicious self-starting code within the browser.
- Attachment quarantine stops suspect email attachments from activating, preventing network-wide virus and worm propagation.
- Privacy enhancement restricts tracking of end-users' surfing history.
- Content controls enable administrators to define lists of keywords and URLs employees are not permitted to access.

Control and Manageability

- Centralized deployment, management and updating provide trouble-free, automated protection and low IT overheads.
- Support for user groups enables different configurations and access policies to be deployed to different users depending on their degree of vulnerability
- Automated spyware and firewall protection keeps client machines functioning smoothly and keeps users productive.
- Firewall presets for commonly-used applications and network-specific communications ease the initial access configuration definitions.

Cost-Efficient Solution

- Combining anti-spyware with a software firewall delivers comprehensive proactive security for the price of a point solution
- Trickle-down updating saves on bandwidth and PC resources.
- ONS is effective right out of the box, with no training or special knowledge required

System Requirements

Minimum hardware specifications:

Central Processor: x-86 compatible processor, 450 Mhz or above

Memory: server-side: 256 Mb; client-side: 128 Mb
Free Disk Space: 50 Mb

Operating system:

Server-side: Windows 2003 Server, Windows 2000, Windows NT
Client-side: Windows XP, Windows 2000, Windows Me, Windows 98

Netsys Solutions

www.netsys.co.in