

Outpost Network Security Datasheet

The Security Challenge for Small Businesses

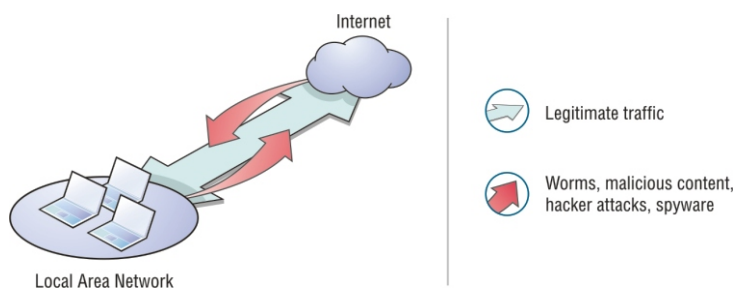
Small businesses don't have the luxury of dedicated IT security staff, but they have just as strong a need for rock-solid protection against the ever-growing threat of Internet-borne attacks from hackers, spyware, and who knows what else. A single attack on a Windows vulnerability before you've had time to patch the operating system can wipe out desktops, leading to financial losses and severely reduced productivity. Threats such as spyware, worms, Trojan horses, hacker exploits and other malicious software can impact companies with anything from bad PR to the loss of critical data.

Small businesses may underestimate the need for protection, believing that their company is too small or insignificant to be a target. Unfortunately, the automated tools and techniques that hackers employ to scan for vulnerable computers mean that no company, whatever its size, is immune.

Endpoint PCs accessing the Internet or communicating over the local network initiate a two-way transmission – information can either leave or enter the computer. Without the right data security management tools, there's no control over just what is being transmitted back and forth – or by whom.

And then there are the mobile PCs taken on business trips - remote connections open up the computer (and the network, when the mobile PC returns to home base) to all manner of unwanted cyber-visitors.

"Nearly 90% of US businesses suffered from a computer virus, spyware or other online attack in 2004 or 2005 despite widespread use of security software" – data taken from the CSI/FBI survey.



The Solution

Control: In an organization where employees have varying degrees of computer experience and different departments or groups of users are governed by different security policies according to risk levels, a central management tool is key to effective control over the security of client systems. This ensures that the job of keeping endpoints secure is owned by the person most qualified for the task; someone who can deploy, manage and update client protection from a global "command center".

Protection: Traditional point solutions such as anti-virus or standalone anti-spyware products are a good foundation, but new threats arise so quickly these days that it's unwise for companies to rely solely on signature-based detection. This type of reactive protection needs to be augmented with proactive defenses that can quarantine potential problems while the vendor is preparing new signatures.

Flexibility: Hardware appliances can provide effective perimeter defenses, but are harder to configure for individual needs and lack the flexibility, control and update features of their software counterparts.

Ease of use: Even the best protection is useless if it's not applied correctly. If the solution is hard to configure, manage, and maintain, there will be problems. Every year, the Computer Security Institute/FBI survey shows that despite all precautions, companies continue to suffer from spyware- and virus-related incidents even after adopting what appear to be adequate security measures because the implementation has been poor.

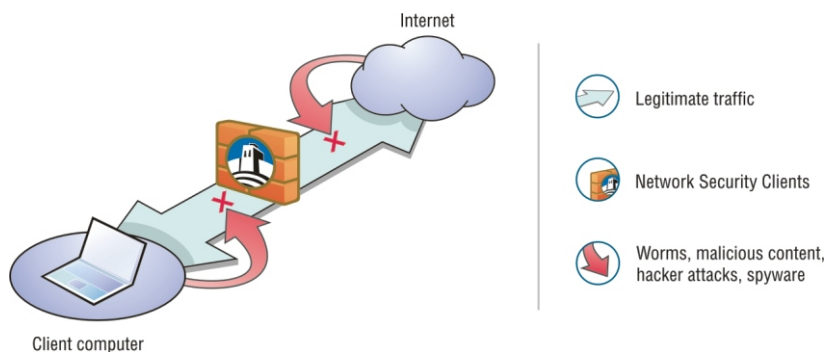
Outpost Network Security

Outpost Network Security (ONS) addresses these concerns by delivering comprehensive protection against today's security challenges that's easy to implement, manage, and maintain. Outpost Network Security incorporates:

- Proven firewall protection
- Proactive and reactive anti-spyware defenses
- Email security
- Content filtering

"The average survival time for an unprotected networked computer dropped from 40 minutes to 20 minutes over the last year."

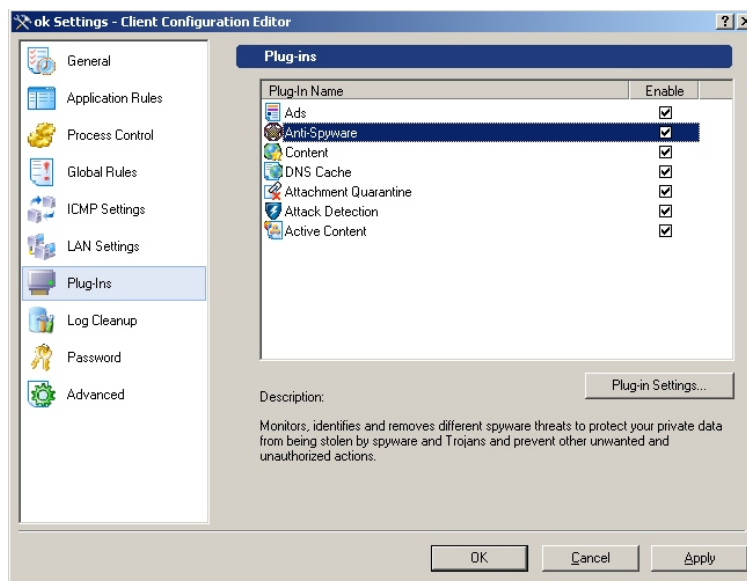
– SANS Institute of Bethesda



Built on the award-winning Outpost Firewall Pro personal firewall and antispysware technology that is the result of years of experience and feedback collected from millions of users, Outpost Network Security provides a superior arsenal of defense for small and mid-sized businesses:

- By enabling centralized deployment, management and updating of client protection remotely from a single console, ONS delivers reliable endpoint security while keeping costs and resource overheads low.
- With its multilayered firewall protection, which incorporates powerful packet- and application- based filtering, stealth technology, intrusion protection, mail attachment quarantine, and privacy protection in an easy-to-use presentation, ONS proactively defends clients against known and unknown threats.
- Built-in spyware protection fights infection at every possible stage – initial contact, infestation, and possible disclosure of data. With tools such as the always-on spyware monitor, the on-demand scanner and the ability to lock down confidential data, the spyware threat is all but eliminated from your network.
- Group support allows administrators to customize protection to fit the security profile of any department or group of users, no matter what their risk profile.
- The automated Agnium Update Service lets administrators download a single client update package and install it across all workstations, cutting down on bandwidth and administrator time. Daily updates of spyware signatures ensure that client machines stay current with the latest protection.

"86% of Computer Crimes originate from inside the company network"
– Intranet Security



Eliminate Security Risks

Outpost Network Security delivers complete protection for all endpoint PCs, automatically deploying and configuring the client firewall across the network to selected workstations. The firewall starts protecting the clients as soon as it is installed by monitoring all data transmissions and applying specific rules for each type of communication.

Total Spyware Defense

Always up-to-date, automated spyware protection prevents infection and keeps clients humming along. The anti-spyware module provides active spyware monitoring and an on-demand scanner, and confidential data can be locked down to prevent it being exported from any client PC either accidentally or deliberately.

Secure Connectivity

Multi-level traffic filtering safeguards your network against unnecessary or malicious connections. By rendering end-user machines invisible on the Internet, hackers cannot locate vulnerable desktops. The Attack Detection module prevents known and unknown attacks on protected workstations, optionally alerting the client. Administrator-assigned application rules govern the client Internet access policy, which can be easily changed on an as-required basis.

Application Integrity

Embedded code control mechanisms stop malicious applications and components from being silently activated under the guise of a trusted program, thus protecting clients from stealthy 'code injection' and spoofing techniques. The Active Web Content module prevents drive-by infections by blocking the installation and/or activation of malicious self-initiating objects. The Attachment Quarantine prevents suspicious email attachments from activating, protecting the network against embedded viruses and worms.

Privacy Shield

The optional privacy enhancement features cloak end users' Internet history, which can protect their computers from certain risks; however, if you wish to track employees' online activities, this function can be disabled.

Productivity and Performance Enhancement

The Ads module blocks banner ads from websites and HTML emails, significantly increasing the speed with which web content can be displayed (as well as removing the temptation to click on those ads). Additionally, the Content module allows administrators to customize blocking of web pages displaying unwanted content.

Low-overhead Management

Outpost Network Security's centralized deployment, management and updating provide trouble-free, automated protection.

Simple Deployment

Client protection can be rolled out from a single administrator console to all or selected workstations. ONS does not need to be installed on a server or domain controller – any dedicated workstation meeting the system requirements can host the Command Center module. Windows Group Policy can be used for automatic client firewall installation in Windows 2000 or later domains.

Centralized Administration

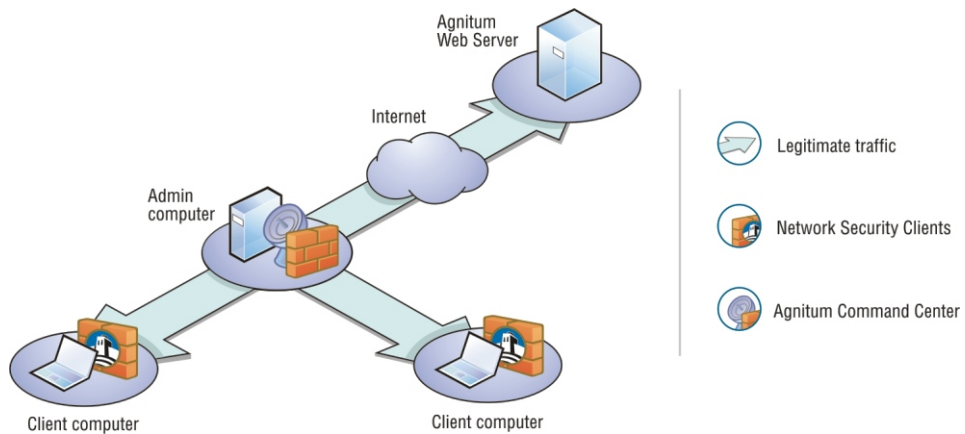
The Agnitum Command Center enables centralized control over individual workstation protection from one location. All management, troubleshooting, and monitoring tasks are performed from this single location, saving the time and effort of visiting individual firewall installations to perform the same operation multiple times.

Fast Updates

The Agnitum Update Service provides scheduled single download, multiple-install client updates, reducing the performance impact on the network by downloading one update and installing it to all clients simultaneously.

Ease of Use

Outpost Network Security provides a familiar user interface, and the Command Center is implemented as an MMC snap-in. The client firewall settings can inherit those of previous Outpost Firewall Pro installations, making the process of configuration easy and fast.



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