

Outpost Office Firewall Product Data Sheet

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

*-SANS Institute
of Bethesda*

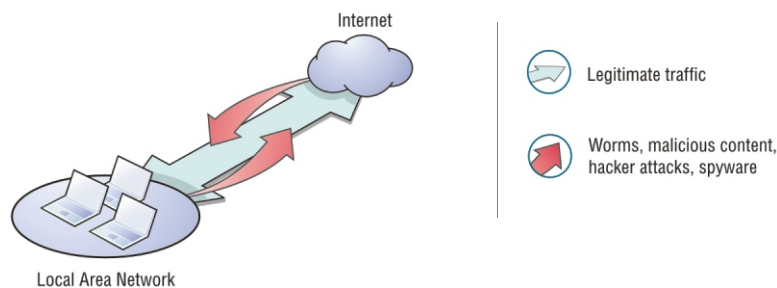
Security Challenge

Every month any of your corporate computers connected to the Internet faces about two hundred new security threats.

Such traditional security measures as antivirus and intrusion detection systems are not enough, especially when malicious code like Slammer worm can propagate in a few minutes before an antiviral signature update is released. In addition you are under threat from spyware agents, remote access Trojans, malicious components embedded into web pages, destructive zombies and distributed hacker attacks.

Because these threats can come from both outside and inside of your network perimeter you cannot underestimate your overall security challenge.

The most threatening fact of all is that those non-stop, automated threats do not recognize whether they face just a small network with a couple of PCs or a large corporation with hundreds of computers.



Your Choice

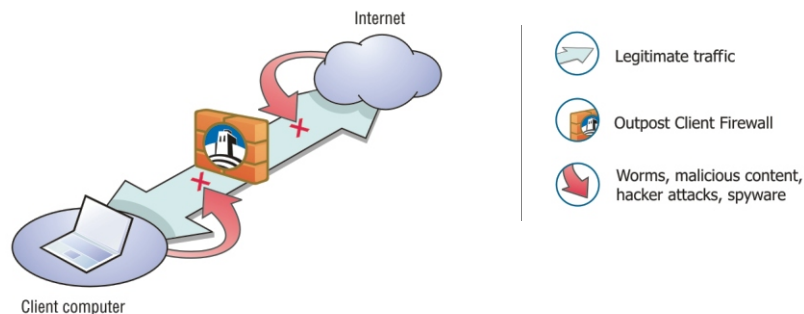
The best possible decision for your corporation is to implement pro-active security measures that do not depend on updates like antivirus and intrusion detection systems. The recommended solution is firewall technology, a solution that constantly monitors and regulates all the traffic enterprise computers receive and send. Unlike antivirus software, a firewall recognizes malicious code not by its "picture" but by its "behavior."

Hardware firewalls are a good choice to start building your security, but they are not so flexible as software firewalls and cannot handle internal threats.

Agnitum's Outpost Office Firewall gives you a cost-effective solution for securing the end-points of your corporate networks from external and internal threats. Outpost Office is based on our best-of-breed personal firewall; it provides a superior arsenal of defense while allowing you to centrally deploy, configure and update the software on each client computer. This makes Outpost Office Firewall the core element of multi-layered protection for modern security measures.

Minimize Risks

Outpost Office Firewall protects your office from all known Internet dangers, automatically deploying and configuring the client firewall across the corporate network on selected workstations. The client firewall starts protecting endpoints as soon as it is installed by monitoring all data that goes in and out and by applying specific rules for each type of data.



Application Filtering

Outpost Office Firewall filters all applications that access the network to send or receive data. Using firewall rules, your network administrators can apply specific security policies by restricting specific ports and protocols for applications. This helps not only to tighten up endpoint security but also prevents network misuse by your employees.

Attack Prevention

The Attack Detection plug-in automatically detects and averts all known Internet attacks against a client computer, allowing flexible per port configuration and providing strong security against hacker intrusions. The firewall provides protection against all known security breaches: it addresses the latest leak tests, ensuring that client protection is complete and rock-solid so that no private data leak is possible.

Malicious Code Protection

By employing technologies of Component Control, Hidden Process Control, and Open Process Control Outpost does not allow malicious applications to be activated as a part of legal programs and thus fully protects clients from Trojans, spyware and other dangers.

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

- Intranet Security

In addition, the Attachment Quarantine plug-in analyzes incoming e-mail for dangerous attachments and renames suspicious attachments. This feature prevents users from occasionally opening harmful files and therefore protects client computers from viruses and worms.

Privacy Shield

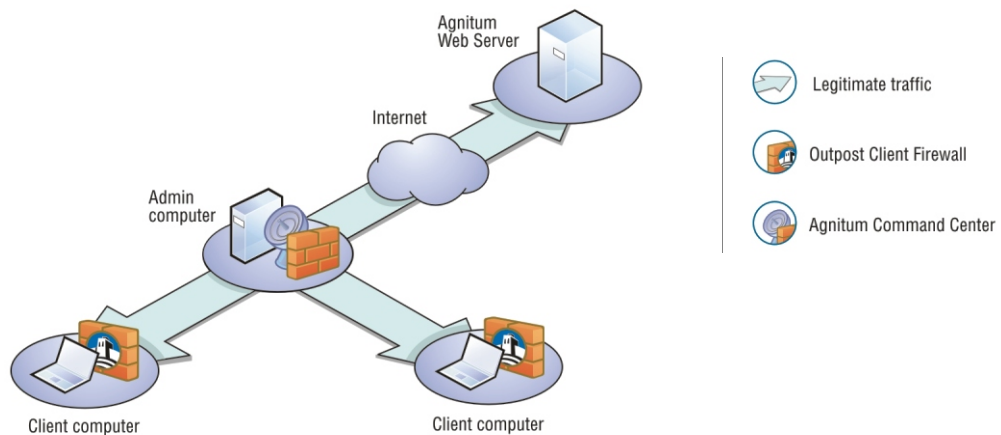
Today any web page visited by your employees can have embedded malicious content. In such cases silent hijacking of just one workstation would cause severe consequences to the entire corporate network. Thanks to the Active Content plug-in the client's privacy is well maintained.

The Active Content plug-in manages active content of web sites that might be harmful to client's system and also protects client web navigation history by flexible blocking referrers and cookies.

Additionally, the Ads plug-in saves clients' time and bandwidth by removing banner ads from sites that they visit; while the Content plug-in allows you to block web pages with objectionable content.

Cost Efficiency

Agnitum Command Center simplifies three major procedures: deployment, administration and updating. This saves time and simplifies traditional tasks performed by your network administrator.



Easy Deployment

Outpost Office Firewall does not have to be installed on a server or domain controller. All the managing tools can be installed on any dedicated workstation that complies with the system requirements. In addition, the product allows for easy mass installation and configuration of workstations across a network, thus saving a lot of administrator time in large and medium companies. You can use Windows Group Policy for automatic client firewall installation in the Windows 2000 or later domain.

Centralized Administration

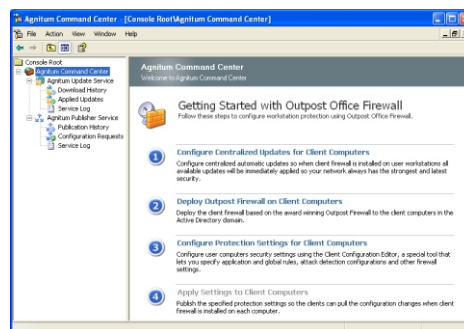
Agnitum Command Center allows control over individual workstation protection from a central location. All management, troubleshooting, and monitoring tasks are performed from a central location, saving administrators time and effort as they avoid visiting each firewall installation and performing the same sets of operations multiple times.

Fast Updates

Agnitum Update Service provides scheduled single download, multi-install client firewall updates, reducing the impact of this Internet traffic on your network bandwidth by downloading one update and installing it to all clients simultaneously.

Ease of Use

Outpost Office Firewall provides a familiar user interface. The main managing application, Agnitum Command Center, is implemented as MMC snap-in. Client firewall settings inherit those of Outpost Firewall and make the process of firewall configuration easy and fast.



System Requirements

Outpost Office Firewall is designed for Microsoft Windows operating systems running on a PC platform. The following are the system requirements for Outpost Office Firewall:

- An Intel Pentium Processor or compatible architecture is required
- Support for the following operating systems:
 - Workstations: Windows 98/ME/2000(SP2)/XP;
 - Servers: Windows NT/2000
- RAM: 32MB
- Microsoft mouse or compatible pointing device
- 256-color VFA monitor or higher
- Internet or Network connection